COMTREND CORPORATION

CT-5361T

Wireless ADSL2+ Router

User Manual

Version A3.6, October 3, 2008

261056-044

Preface

This manual provides information related to the installation, operation, and application of this device. The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

If you find the product to be inoperable or malfunctioning, please contact technical support for immediate service by email at INT-support@comtrend.com

For product update, new product release, manual revision, or software upgrades, please visit our website at http://www.comtrend.com

Important Safety Instructions

With reference to unpacking, installation, use, and maintenance of your electronic device, the following basic guidelines are recommended:

- Do not use or install this product near water, to avoid fire or shock hazard. For example, near a bathtub, kitchen sink or laundry tub, or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).
- Do not connect the power supply cord on elevated surfaces. Allow it to lie freely. There should be no obstructions in its path and no heavy items should be placed on the cord. In addition, do not walk on, step on, or mistreat the cord.
- Use only the power cord and adapter that are shipped with this device.
- To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are not blocked.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening. Also, do not use the telephone to report a gas leak in the vicinity of the leak.
- Never install telephone wiring during stormy weather conditions.

CAUTION:

- To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.
- Always disconnect all telephone lines from the wall outlet before servicing or disassembling this equipment.

WARNING

- Disconnect the power line from the device before servicing.
- Power supply specifications are clearly stated in Appendix C.

Copyright

Copyright©2008 Comtrend Corporation. All rights reserved. The information contained herein is proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of Comtrend Corporation.

NOTE:	This document is subject to change without notice.

Table of Contents

CHAPTER 1 INTRODUCTION 4
1.1 FEATURES 4
1.2 APPLICATION 4

CHAPTER 2 INSTALLATION 5
2.1 HARDWARE SETUP 5
2.2 USB DEVICE DRIVER AUTO-RUN INSTALLATION 6
2.3 USB DRIVER MANUAL INSTALLATION (64BIT OS) 9
2.4 LED INDICATORS 14

CHAPTER 3 WEB USER INTERFACE 15
3.1 DEFAULT SETTINGS 15
3.2 IP CONFIGURATION 16
3.3 LOGIN PROCEDURE 17

CHAPTER 4 QUICK SETUP 19
4.1 AUTO QUICK SETUP 20
4.2 MANUAL QUICK SETUP 21
4.2.1 PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE) 23
4.2.2 MAC Encapsulation Routing (MER) 27
4.2.3 IP Over ATM 30
4.2.4 Bridging 33

CHAPTER 5 DEVICE INFORMATION 35
5.1 WAN 36
5.2 STATISTICS 36
5.2.1 LAN Statistics 36
5.2.2 WAN Statistics 37
5.2.3 ATM statistics 38
5.2.4 ADSL Statistics 40
5.3 ROUTE 43
5.4 ARP 44
5.5 DHCP 44

CHAPTER 6 ADVANCED SETUP 45
6.1 WAN 45
6.2 LAN 46
6.3 NAT 48
6.3.1 Virtual Servers 48
6.3.2 Port Triggering 49
6.3.3 DMZ Host 51
6.3.4 ALG 51
6.4 SECURITY 52
6.4.1 IP Filtering 52
6.4.2 MAC Filtering 54
6.4.3 Parental Control 56
6.5 QUALITY OF SERVICE 57
6.6 ROUTING 59
6.6.1 Default Gateway 59
6.6.2 Static Route 60
6.6.3 RIP 60
6.7 DNS 61
6.7.1 DNS Server 61
6.7.2 Dynamic DNS 61
6.8 DSL 63
6.9 PORT MAPPING 64
6.10 CERTIFICATE 66
6.10.1 Local 66
6.10.2 Trusted CA 68

CHAPTER 7 WIRELESS 69
7.1 BASIC 69
7.2 SECURITY 70
7.3 MAC FILTER 72
7.4 WIRELESS BRIDGE 73
7.5 ADVANCED 74
7.6 QUALITY OF SERVICE 76
7.7 STATION INFO 77
CHAPTER 8 DIAGNOSTICS 78
CHAPTER 9 MANAGEMENT 80
9.1 SETTINGS 80
9.1.1 Backup Settings 80
9.1.2 Update Settings 80
9.1.3 Restore Default 81
9.2 SYSTEM LOG 82
9.3 SNMP AGENT 83
9.4 TR-069 CLIENT 84
9.5 INTERNET TIME 85
9.6 ACCESS CONTROL 86
9.6.1 Services 86
9.6.2 IP Addresses 86
9.6.3 Passwords 87
9.7 UPDATE SOFTWARE 88
9.8 SAVE AND REBOOT 89
APPENDIX A: FIREWALL 90
APPENDIX B: PIN ASSIGNMENTS 94
APPENDIX C: SPECIFICATIONS 95
APPENDIX D: SSH CLIENT 97

Chapter 1 Introduction

The CT-5361T Wireless ADSL2+ Router is designed for both residential and business applications that require wired and wireless connectivity to an ADSL broadband network. In terms of connectivity, it comes fully equipped with four Fast Ethernet ports , a single USB port and an integrated 802.11g WiFi WLAN Access Point (AP) for wireless connectivity. The TR-068 compliant front and rear panels are another key feature which make the CT-5361T easy to setup and use.

The CT-5361T supports up to 16 contiguous virtual connections allowing for multiple simultaneous Internet connections. It also provides state of the art security with WPA data encryption, Firewall and VPN with pass through (PPTP/L2TP/IPSec). TR-069 compliance allows for auto configuration and control via a remote ACS.

1.1 Features

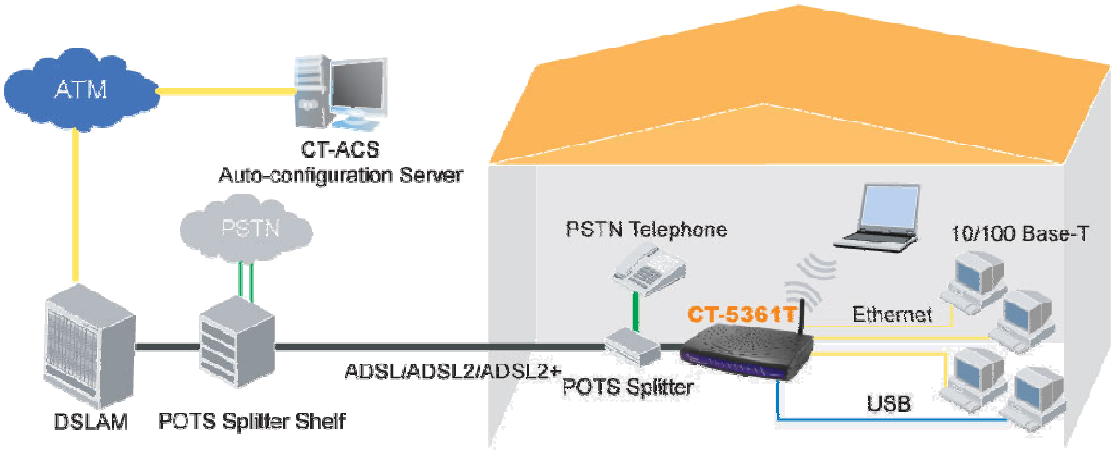
- UPnP
- Static route and RIP v1/v2 routing
- IP/ATM QoS
- IGMP Proxy/Snooping
- DNS Proxy
- Per-VC packet level QoS
- Embedded SNMP agent
- Remote administration and upgrade
- FTP/TFTP server
- RADIUS client
- IP/MAC address filtering
- Dynamic IP assignment
- NAT/PAT
- DHCP Server/Relay/Client
- Auto PVC configuration
- Up to 16 VCs
- Web-based management
- Configuration backup and restoration
- TR-068 compliant
- 802.1q/802.1p
- Supports TR-069/TR-098/TR-111 remote management protocols

WIRELESS

- Integrated 802.11b/g AP
- Optional Turbo mode (Afterburner)
- WPA/WPA2 and 802.1x
- WMM

1.2 Application

The following diagram depicts the application of the CT-5361T.

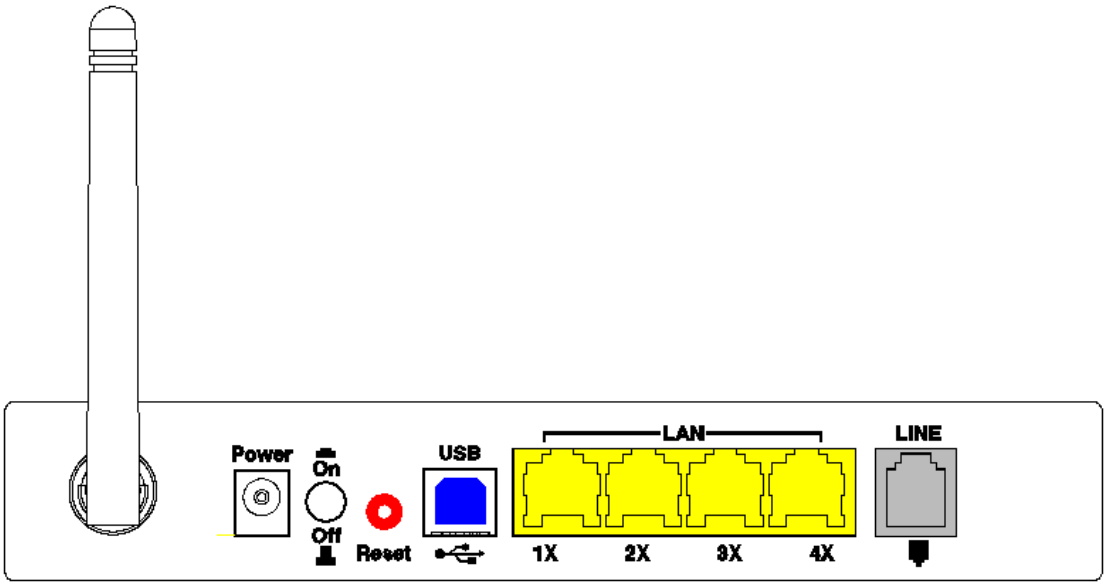


Chapter 2 Installation

2.1 Hardware Setup

Follow the instructions below to complete the hardware setup.

The diagram below shows the back panel of the device.



Power ON
Press the power button to the OFF position (OUT). Connect the power adapter to the power port. Attach the power adapter to a wall outlet or other AC source. Press the power button to the ON position (IN). The Power LED indicator should light up (GREEN). The device first performs a POST (Power On Self Test). If the POST fails, the LED will turn RED. Wait a few moments for the test to finish. If the light is a steady GREEN, the device is ready for setup.

Caution 1: If the device fails to power up, or it malfunctions, first verify that the power cords are connected securely. Then power it on again. If the problem persists, contact technical support.

Caution 2: Before servicing or disassembling this equipment, disconnect all power cords and telephone lines from their outlets.

Reset Button
Restore the default parameters of the device by pressing the Reset button for 5 to 10 seconds. After the device has rebooted successfully, the front panel should display as expected (see section 2.4 LED Indicators for details).

NOTE: If pressed down for more than 12 seconds, the CT-5361T will go into a firmware update state (CFE boot mode). The firmware can then be updated using an Internet browser pointed to the default IP address.

Connection to USB
Before connecting the CT-5361T to a PC with the USB cable, the USB device driver must first be installed. See the sections 2.2 and 2.3 for detailed instructions.

Connection to LAN
Use RJ45 cable to connect up to four network devices. These ports are auto-sensing MDI/X and either straight-through or crossover cable can be used.

Connection to LINE
Connect the ADSL line to this port with a RJ11 cable.

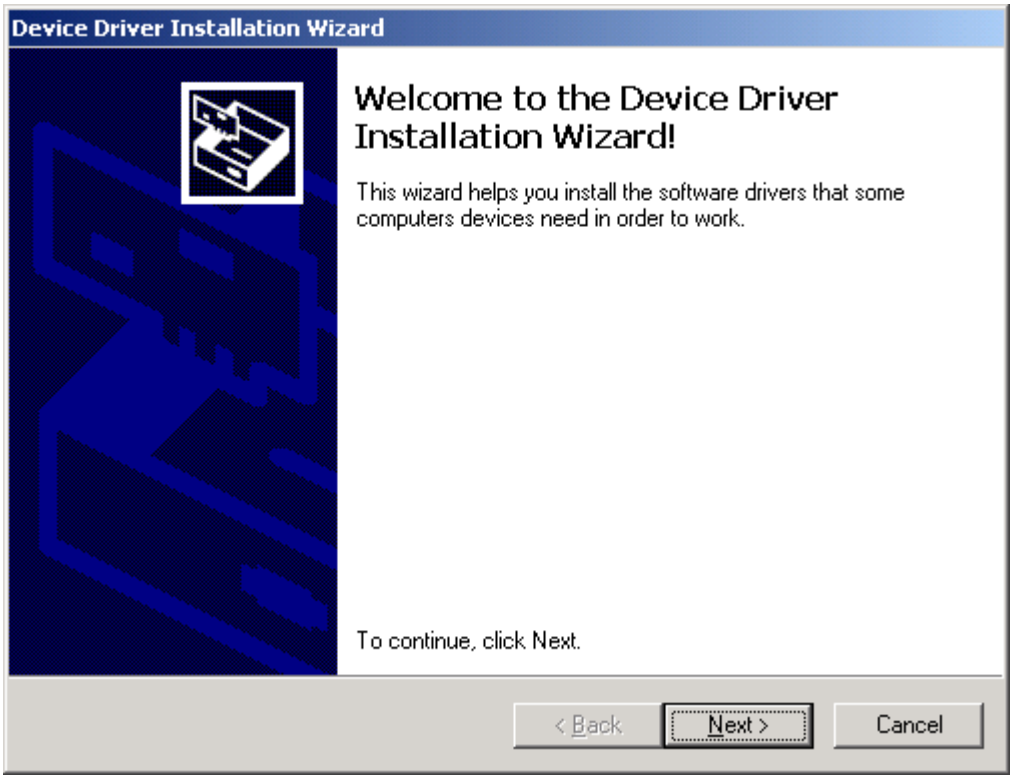
2.2 USB Device Driver Auto-run Installation

Before connecting the CT-5361T to a PC with USB, the correct drivers must be installed. The auto-run USB driver installation supports Win ME, Win 98, Win 2000, Win XP (32 bit) and Vista (32 bit). For those using Windows XP 64 bit, the driver must be installed manually (please see the following section for details).

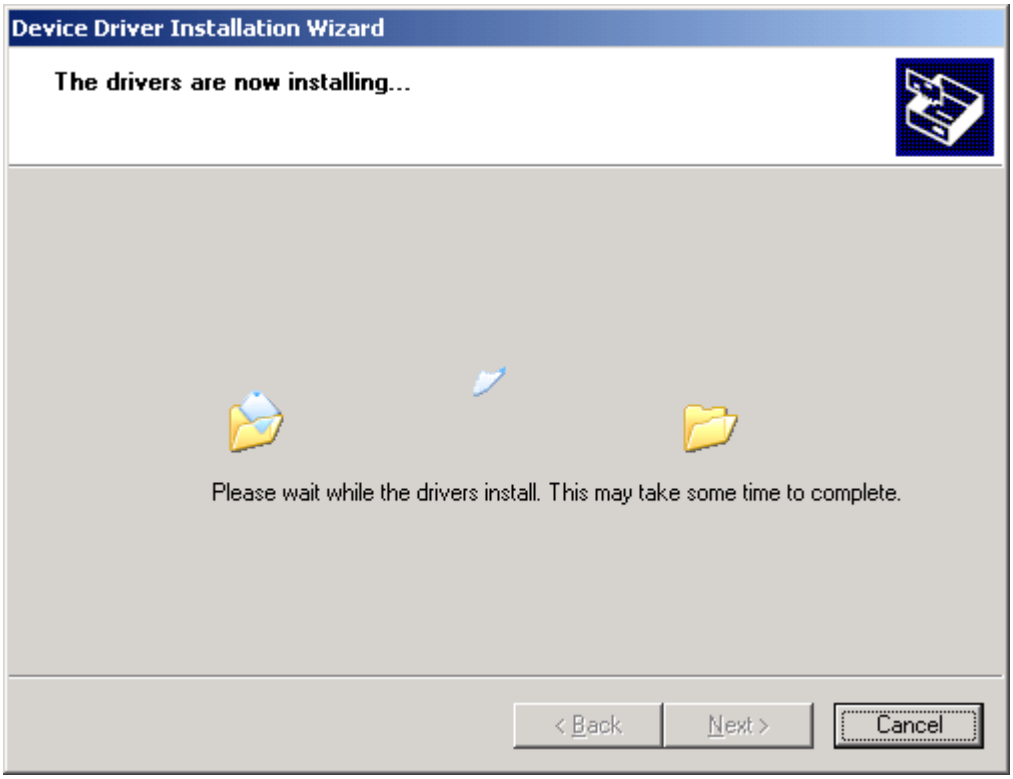
Follow the procedure below to install the standard (32 bit) USB driver

STEP 1: Insert the Installation CD and select **Install USB Driver** from the autostart menu shown below.

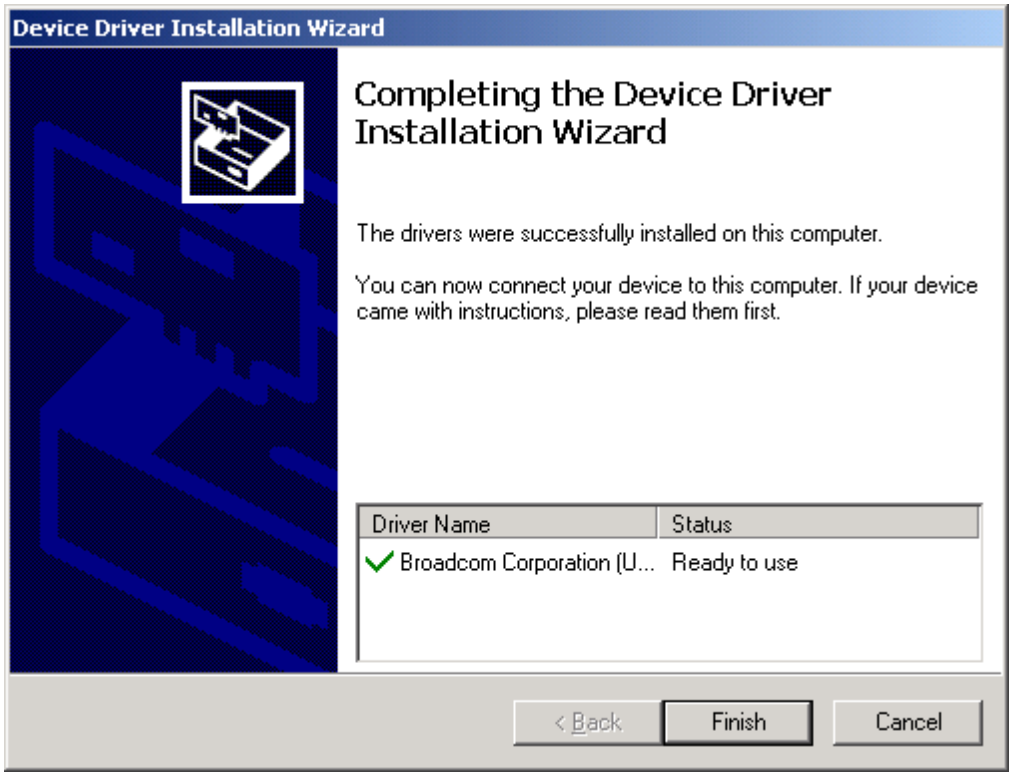
STEP 2: The following window will display. Click **Next** to continue.


Device Driver Installation Wizard
Welcome to the Device Driver Installation Wizard!
This wizard helps you install the software drivers that some computers devices need in order to work.
To continue, click Next.
< Back
Next >
Cancel

STEP 3: When the window displays as below, wait for the drivers to fully install.


Device Driver Installation Wizard
The drivers are now installing...
Please wait while the drivers install. This may take some time to complete.
< Back
Next >
Cancel

STEP 4: Click **Finish**, when the window displays as below.


Device Driver Installation Wizard
Completing the Device Driver Installation Wizard
The drivers were successfully installed on this computer.
You can now connect your device to this computer. If your device came with instructions, please read them first.
Driver Name
Status
Broadcom Corporation (U...
Ready to use
< Back
Finish
Cancel

STEP 5: Installation is complete. Now connect the device to your PC using standard USB cable.

2.3 USB Driver Manual Installation (64bit OS)

Before connecting this router to a PC with USB, the correct drivers must be installed.

Follow the procedure below to manually install the 64-bit USB driver

STEP 1: Connect the USB port to the PC by plugging the flat connector of a standard USB cable into your PC and plugging the square connector into the device. After a moment, the connection should be detected by your PC and if so, the screen will display a notice to that effect, as shown below:

STEP 2: When the window displays as below, select **Install from a list or specific location (Advanced),** and then click the **Next** button.

Found New Hardware Wizard
Welcome to the Found New Hardware Wizard
This wizard helps you install software for:
USB Network Interface
If your hardware came with an installation CD or floppy disk, insert it now.
What do you want the wizard to do?
Install the software automatically (Recommended)
Install from a list or specific location (Advanced)
Click Next to continue.
< Back
Next >
Cancel

NOTE:	This window won't display if the USB Driver has been previously installed. In this case, contact technical support for assistance.

STEP 3: Insert the installation CD.

NOTE:	If you see the autostart menu (as shown in **step 1** of previous section) **CLICK -** Exit and continue with the manual installation process.

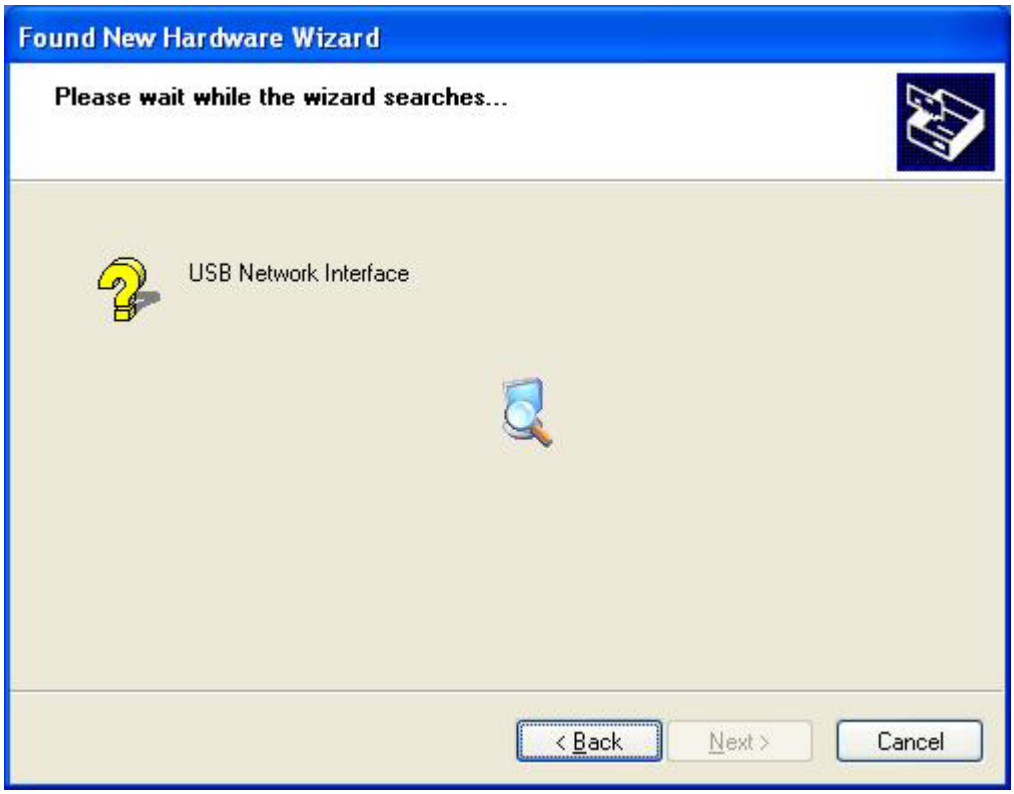
Found New Hardware Wizard
Please choose your search and installation options.
Search for the best driver in these locations.
Use the check boxes below to limit or expand the default search, which includes local paths and removable media. The best driver found will be installed.
Search removable media (floppy, CD-ROM...)
Include this location in the search:
Browse
Don't search. I will choose the driver to install.
Choose this option to select the device driver from a list. Windows does not guarantee that the driver you choose will be the best match for your hardware.
< Back
Next >
Cancel

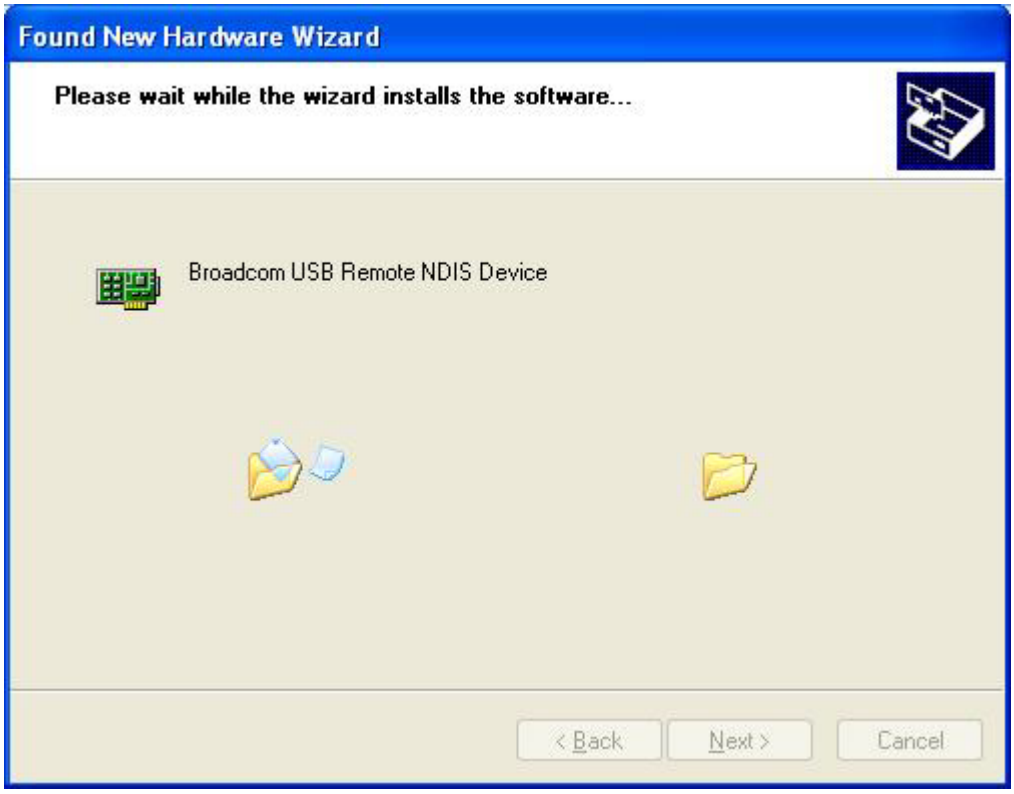
STEP 4: Select the location of the file using the **Browse** button, as shown above. Normally, the file is on the CD-ROM shipped with the device.

STEP 5: Locate the **Vista** folder, and click **OK**.

STEP 6: When the window displays as below, click **Next,** and then wait.

Found New Hardware Wizard
Please choose your search and installation options.
Search for the best driver in these locations.
Use the check boxes below to limit or expand the default search, which includes local paths and removable media. The best driver found will be installed.
Search removable media (floppy, CD-ROM...)
Include this location in the search:
E:\Vista
Browse
Don't search. I will choose the driver to install.
Choose this option to select the device driver from a list. Windows does not guarantee that the driver you choose will be the best match for your hardware.
< Back
Next >
Cancel


Found New Hardware Wizard
Please wait while the wizard searches...
USB Network Interface
< Back
Next >
Cancel



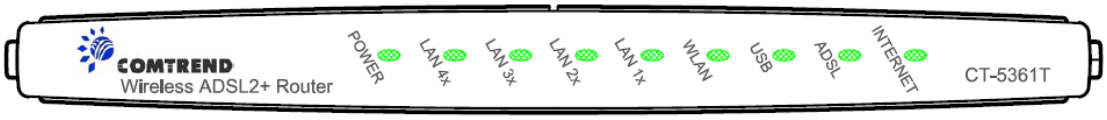
STEP 7: Click the **Finish** button when the window displays as below.

Found New Hardware Wizard
Completing the Found New Hardware Wizard
The wizard has finished installing the software for:
Broadcom USB Remote NDIS Device
Click Finish to close the wizard.
< Back
Finish
Cancel

STEP 8: Installation is complete. You can now use the USB connection.

2.4 LED Indicators

The front panel LED indicators are shown below and explained in the following table. This information can be used to check the status of the device and its connections.



LED	Color	Mode	Function
POWER	Green	On	The device is powered up.
		Off	The device is powered down.
	Red	On	POST (Power On Self Test) failure or other malfunction. A malfunction is any error of internal sequence or state that will prevent the device from connecting to the DSLAM or passing customer data.
LAN 4x-1x	Green	On	An Ethernet Link is established.
		Off	An Ethernet Link is not established.
		Blink	Data transmitting or receiving over LAN.
WLAN	Green	On	The wireless module is ready and idle.
		Off	The wireless module is not installed.
		Blink	Data transmitting or receiving over WLAN.
USB	Green	On	A USB link is established.
		Off	A USB link is not established.
		Blink	Data transmitting or receiving over USB.
ADSL	Green	On	The ADSL link is established.
		Off	The ADSL link is not established.
		Blink	The ADSL link is training.
INTERNET	Green	On	IP connected and no traffic detected. If an IP or PPPoE session is dropped due to an idle timeout, the light will remain green if an ADSL connection is still present.
		Off	Modem power off, modem in bridged mode or ADSL connection not present. In addition, if an IP or PPPoE session is dropped for any reason, other than an idle timeout, the light is turned off.
		Blink	IP connected and IP Traffic is passing thru the device (either direction)
	Red	On	Device attempted to become IP connected and failed (no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.)

Chapter 3 Web User Interface

This section describes how to access the device via the web user interface (WUI) using an Internet browser such as Internet Explorer (version 5.0 and later).

3.1 Default Settings

The factory default settings of this device are summarized below.

- LAN IP address: 192.168.1.1
- LAN subnet mask: 255.255.255.0
- Administrative access (username: **root** , password: **12345**)
- User access (username: **user**, password: **user**)

- DHCP server: **enabled** in routing modes (PPPoA/E, IPoA & MER)

- Firewall and NAT: **enabled** for PPPoE and PPPoA
  disabled for Bridge*, MER and IPoA
  (* NAT is not available in Bridge mode)

- Remote WAN access: **disabled**
- Remote (WAN) access (username: **support**, password: **support**)
- WAN IP address: none

- WLAN access: **enabled** (SSID = Comtrend6677)

This device supports the following connection types.

- PPP over Ethernet (PPPoE)
- PPP over ATM (PPPoA)
- MAC Encapsulated Routing (MER)
- IP over ATM (IPoA)
- Bridging

Technical Note:
During power on, the device initializes all settings to default values. It will then read the configuration profile from the permanent storage section of flash memory. The default attributes are overwritten when identical attributes with different values are configured. The configuration profile in permanent storage can be created via the web user interface or telnet user interface, or other management protocols. The factory default configuration can be restored either by pushing the reset button for more than five seconds until the power indicates LED blinking or by clicking the Restore Default Configuration option in the Restore Settings screen.

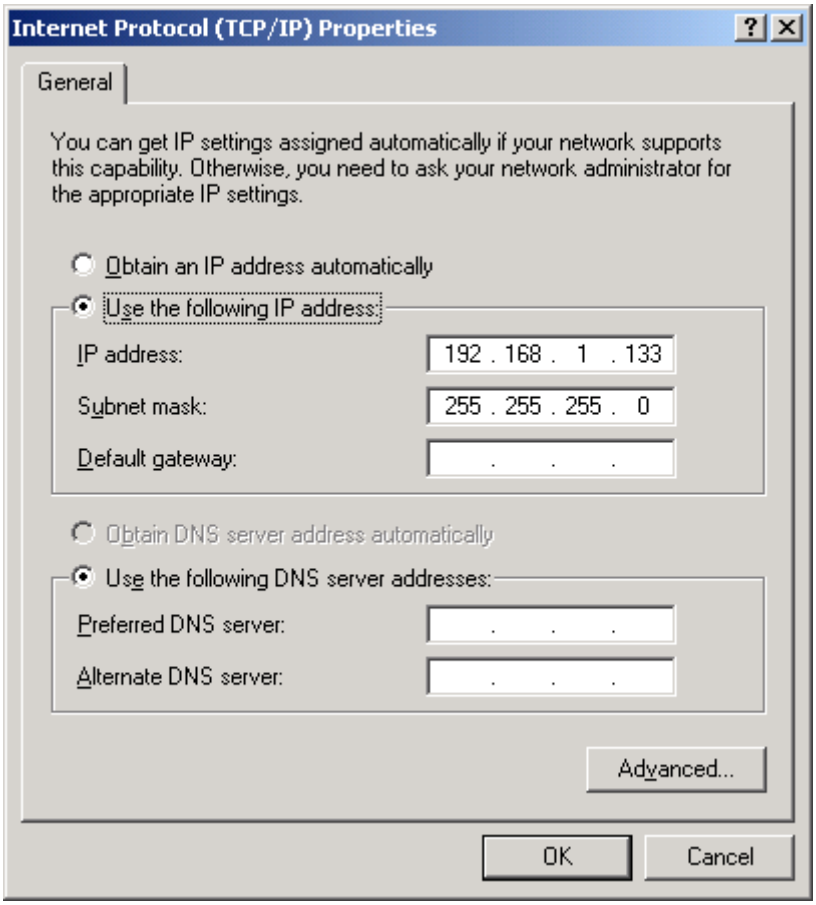
3.2 IP Configuration

STATIC IP MODE

To access router settings, your PC must have a static IP address within the 192.168.1.x subnet. Follow the steps below to configure your PC IP address to use subnet 192.168.1.x. The following steps assume you are running Windows XP.

STEP 1: From the Network Connections window, open Local Area Connection (*You may also access this screen by double-clicking the Local Area Connection icon on your taskbar*). Click the **Properties** button.

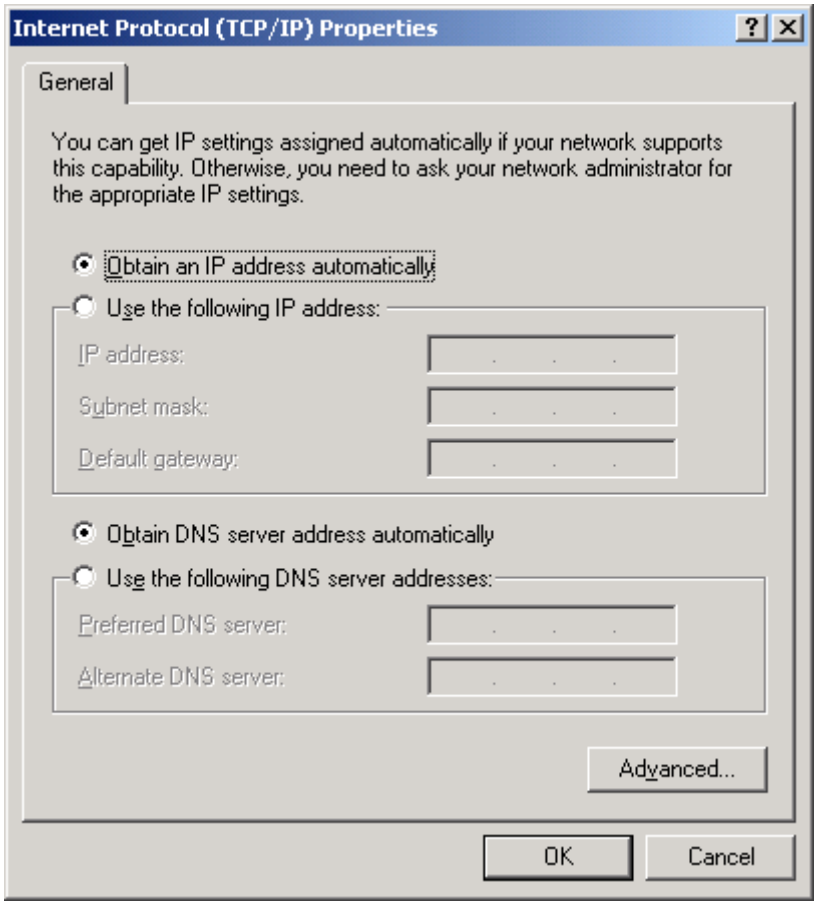
STEP 2: **Select Internet Protocol (TCP/IP)** and click the **Properties** button. The screen should now display as below. Change the IP address to the domain of 192.168.1.x (1<x<254) with subnet mask of 255.255.255.0.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 1 . 133
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

STEP 3: Click **OK** to submit the settings.

DHCP MODE

Set your PC to DHCP mode by selecting **Obtain an IP address automatically** in the Internet Protocol Properties dialog box, as shown below.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

3.3 Login Procedure

Perform the following steps to login to the web user interface.

NOTE:	The default settings can be found in 3.1 Default Settings.

STEP 1: Start the Internet browser and enter the default IP address for the device in the Web address field. For example, if the default IP address is 192.168.1.1, type http://192.168.1.1.

NOTE:	For local administration (i.e. LAN access), the PC running the browser must be attached to the Ethernet, and not necessarily to the device. For remote access (i.e. WAN), use the IP address shown on the Device Info - WAN screen and login with remote username and password.

STEP 2: A dialog box will appear, such as the one below. Enter a default username and password, as defined in section 3.1 Default Settings.

Click **OK** to continue.

NOTE:	The login password can be changed later (see 9.6.3 Passwords)

STEP 3: After successfully logging in for the first time, you will reach this screen.

NOTE1:	If a PVC connection already exists then this Quick Setup screen will be bypassed and the Device Info – Summary screen will display instead.
NOTE2:	The selections available on the main menu (onscreen at left) are based upon the configured connection and user account privileges.

Chapter 4 Quick Setup

The function allows the user to configure the ADSL router for DSL connectivity and Internet access. It guides the user though the WAN network setup first and then the LAN interface setup. The user can either manually customize the router or follow the auto quick setup procedure.

The following configuration considerations apply:

- The WAN network operating mode operation depends on the service provider's configuration on the Central Office side and Broadband Access Server for the PVC
- If the service provider provides PPPoE service, then the connection selection depends on whether the LAN-side device (typically a PC) is running a PPPoE client or whether the CT-5361T is to run the PPPoE client. The CT-5361T can support both cases simultaneously.
- If some or none of the LAN-side devices are not running a PPPoE client, then select PPPoE. If all LAN-side devices are running PPPoE clients, then select Bridge In PPPoE mode, CT-5361T also supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client from non-PPPoE LAN devices.
- NAT and firewall are always enabled when PPPoE mode is selected, but they can be enabled or disabled by the user when MER or IPoA is selected, NAT and firewall are always disabled when Bridge mode is selected.
- Depending on the network-operating mode, and NAT and firewall status, the main menu will display or hide the NAT/Firewall menu. For instance, if the default network-operating mode is Bridge, the main menu will not show the NAT and Firewall menu.

NOTE:	Up to 16 PVC profiles can be configured and saved in the flash memory. To activate a particular PVC profile, you must navigate through all the setup screens until the last summary screen, and click **Save/Reboot**.

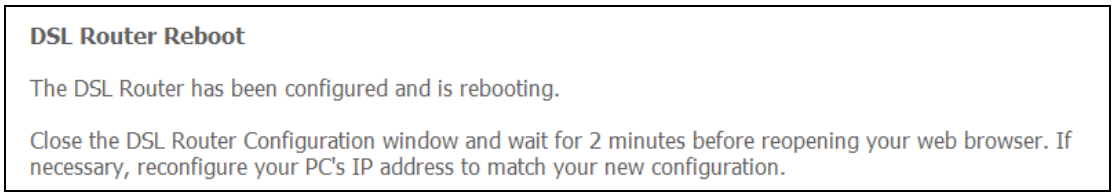
4.1 Auto Quick Setup

The auto quick setup procedures require the ADSL link to be up to automatically detect PVCs. You simply need to follow the online instructions as prompted.

Step 1: Select Quick Setup to display the DSL Quick Setup screen.

Step 2: Click **Next** to start the setup process. Follow the online instructions to complete the setting. This procedure will skip some advanced setup procedures (such as PVC index and encapsulation selection).

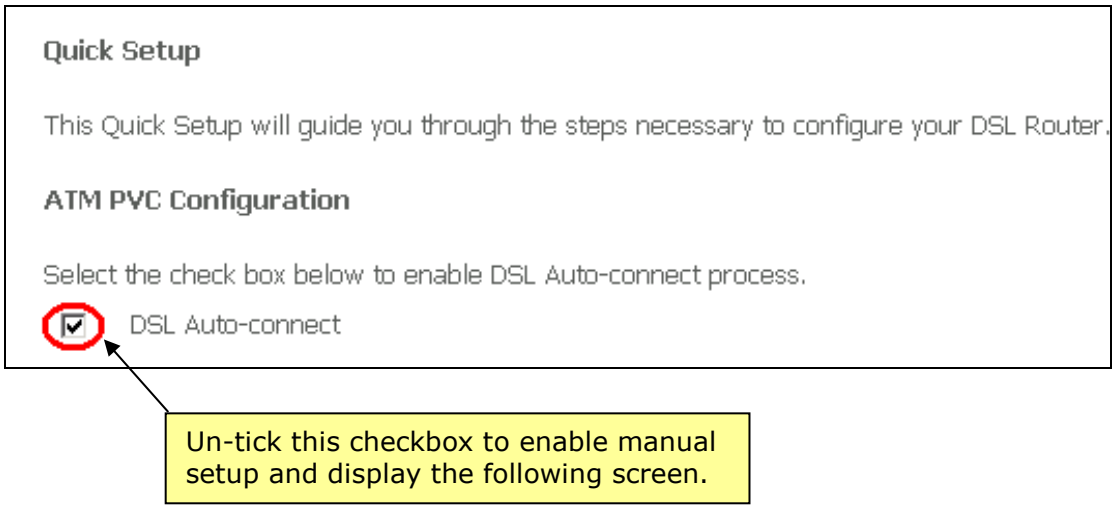
Step 3: After the setup is complete the CT-5361T will reboot.

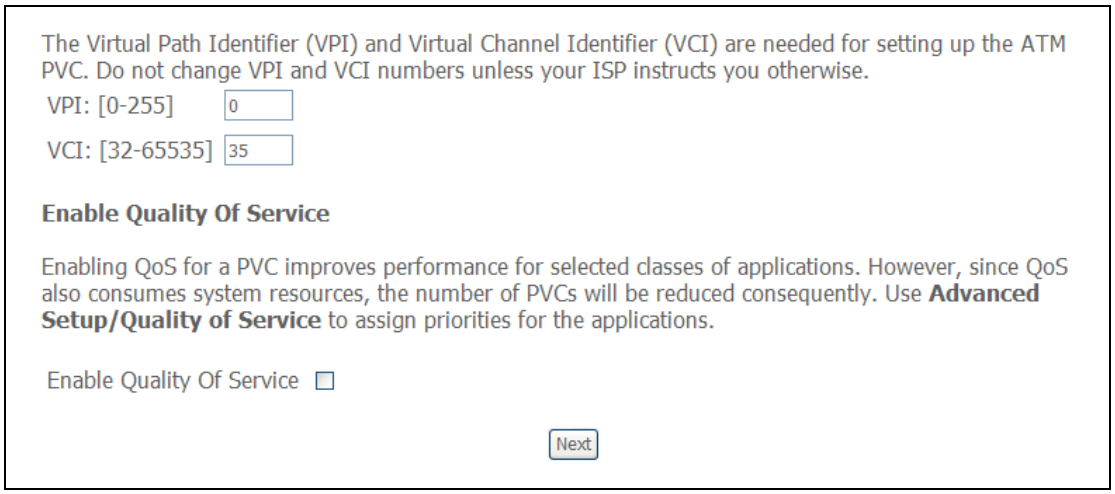

DSL Router Reboot
The DSL Router has been configured and is rebooting.
Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

NOTE: After the device reboots, the Device Info – Summary screen should appear. If the browser does not refresh automatically, close it and restart. You will need to login again.

4.2 Manual Quick Setup

STEP 1: Click **Quick Setup** and un-tick the **DSL Auto-connect** checkbox ☑ to enable manual configuration of the connection type.


Quick Setup
This Quick Setup will guide you through the steps necessary to configure your DSL Router.
ATM PVC Configuration
Select the check box below to enable DSL Auto-connect process.
DSL Auto-connect
Un-tick this checkbox to enable manual setup and display the following screen.

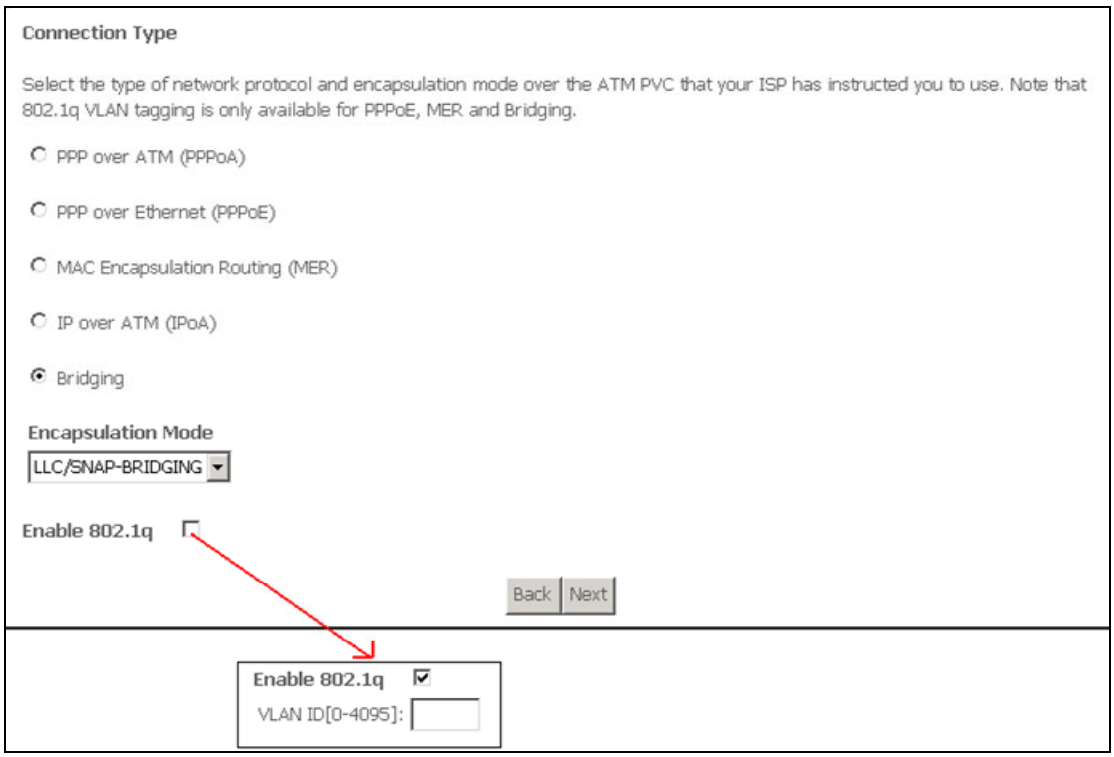

The Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) are needed for setting up the ATM PVC. Do not change VPI and VCI numbers unless your ISP instructs you otherwise.
VPI: [0-255] 0
VCI: [32-65535] 35
Enable Quality Of Service
Enabling QoS for a PVC improves performance for selected classes of applications. However, since QoS also consumes system resources, the number of PVCs will be reduced consequently. Use Advanced Setup/Quality of Service to assign priorities for the applications.
Enable Quality Of Service
Next

STEP 2: Adjust the VPI/VCI settings for the connection you wish to establish. You may also **Enable Quality of Service** (QoS) with its checkbox ☑.

STEP 3: On this screen, you can choose the connection type and select the appropriate encapsulation mode. The available options are shown.

- PPPoA- VC/MUX, LLC/ENCAPSULATION
- PPPoE- LLC/SNAP BRIDGING, VC/MUX
- MER- LLC/SNAP-BRIDGING, VC/MUX
- IPoA- LLC/SNAP-ROUTING, VC MUX
- Bridging- LLC/SNAP-BRIDGING, VC/MUX

You may also choose to **Enable 802.1q** (available in PPPoE, MER and Bridging modes) and enter the VLAN ID, as shown below.

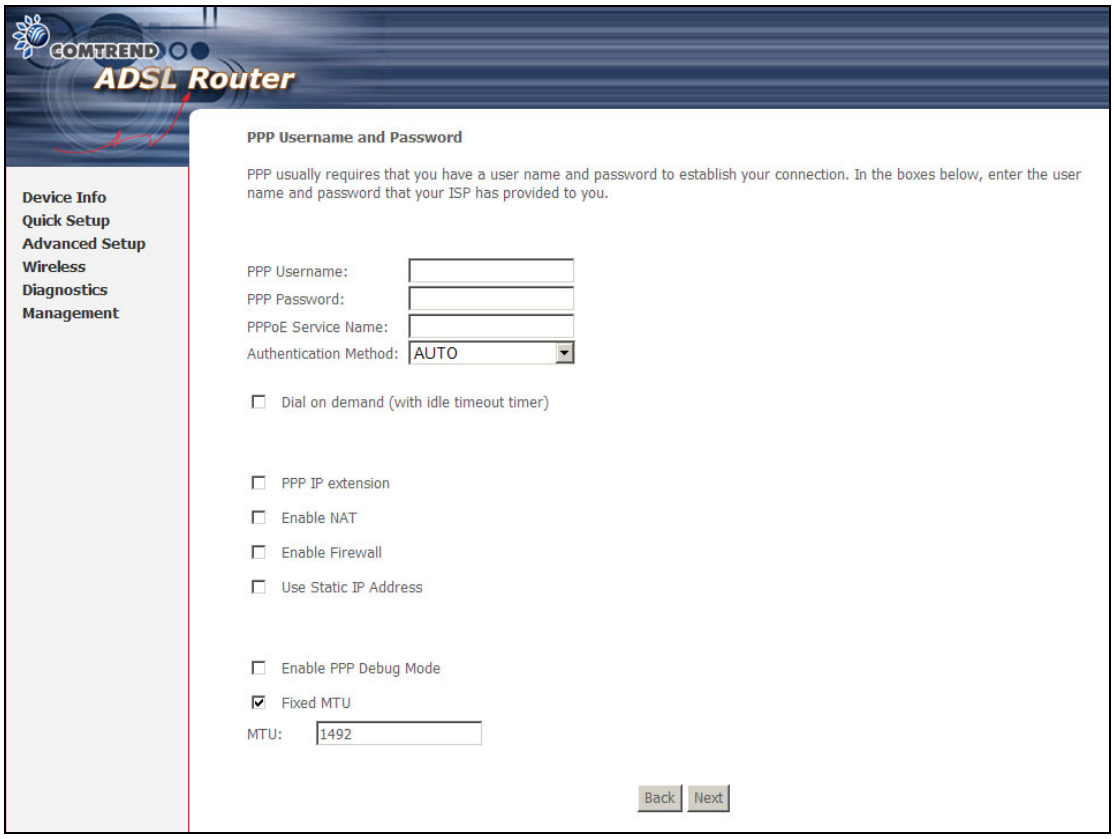

Connection Type
Select the type of network protocol and encapsulation mode over the ATM PVC that your ISP has instructed you to use. Note that 802.1q VLAN tagging is only available for PPPoE, MER and Bridging.
PPP over ATM (PPPoA)
PPP over Ethernet (PPPoE)
MAC Encapsulation Routing (MER)
IP over ATM (IPoA)
Bridging
Encapsulation Mode
LLC/SNAP-BRIDGING
Enable 802.1q
Back
Next
Enable 802.1q
VLAN ID[0-4095]:

Click **Next** to continue…

NOTE:	The subsections that follow continue the ATM PVC setup procedure. Enter the appropriate settings for your service. Choosing different connection types will lead to a different sequence of setup screens.

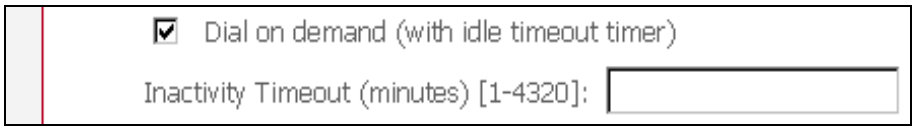
4.2.1 PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE)

STEP 4: Enter the PPP settings as provided by your ISP.



PPP Settings
The PPP Username, PPP password and the PPPoE Service Name entries are dependent on the particular requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. For Authentication Method, choose from AUTO, PAP, CHAP, and MSCHAP.

Dial on Demand
The CT-5361T can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** check box. When the checkbox ☑ is ticked, you must enter an inactivity timeout period of 1 to 4320 minutes.



PPP IP Extension
The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specifically requires this setup, do not select it.

PPP IP Extension does the following:

- Allows only one PC on the LAN
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the

device has only a single IP address to assign to a LAN device.

- NAT and firewall are disabled when this option is selected.
- The device becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The device extends the IP subnet at the remote service provider to the LAN PC. i.e. the PC becomes a host belonging to the same IP subnet.
- The device bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the device's LAN IP address.

Enable NAT
If the LAN is configured with a private IP address, the user should select this checkbox ☑. The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox ☑ should not be selected, so as to free up system resources for improved performance.

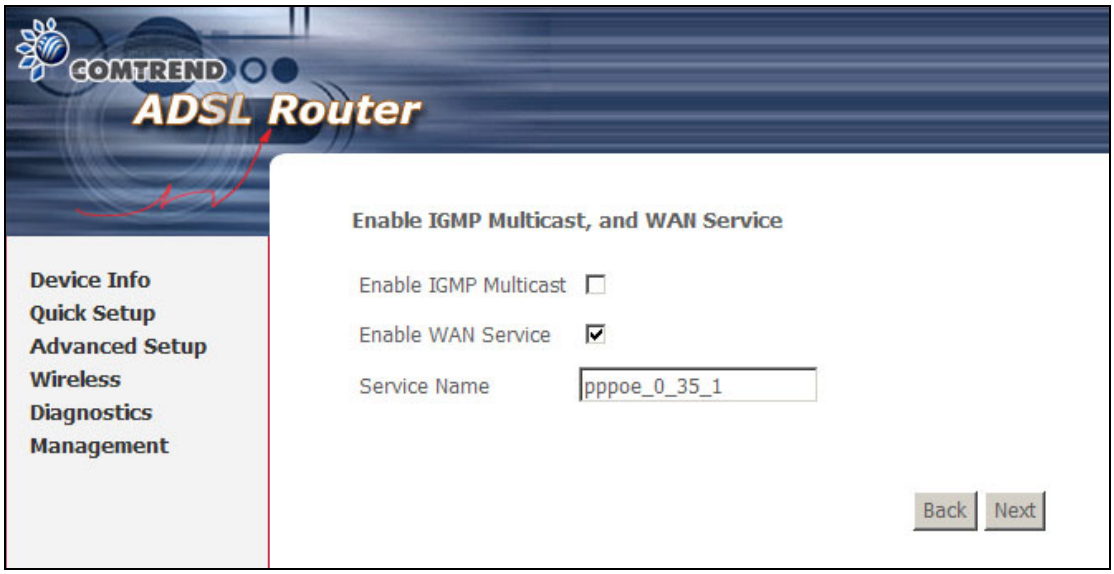
Enable Firewall
If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should be de-selected to free up system resources for better performance.

Use Static IP Address
Unless your service provider specially requires this setup, do not select it.
If selected, enter your static IP address in the IP Address field.

Enable PPP Debug Mode
When this option is selected, the system will put more PPP connection information into the system log. This is for debugging errors and not for normal usage.

Fixed MTU
This option allows us to change the MTU size for WAN interface, PPPoE and PPPoA. The default value is 1492 for PPPoE and 1500 for PPPoA.

STEP 5: Click **Next** to display the following screen.

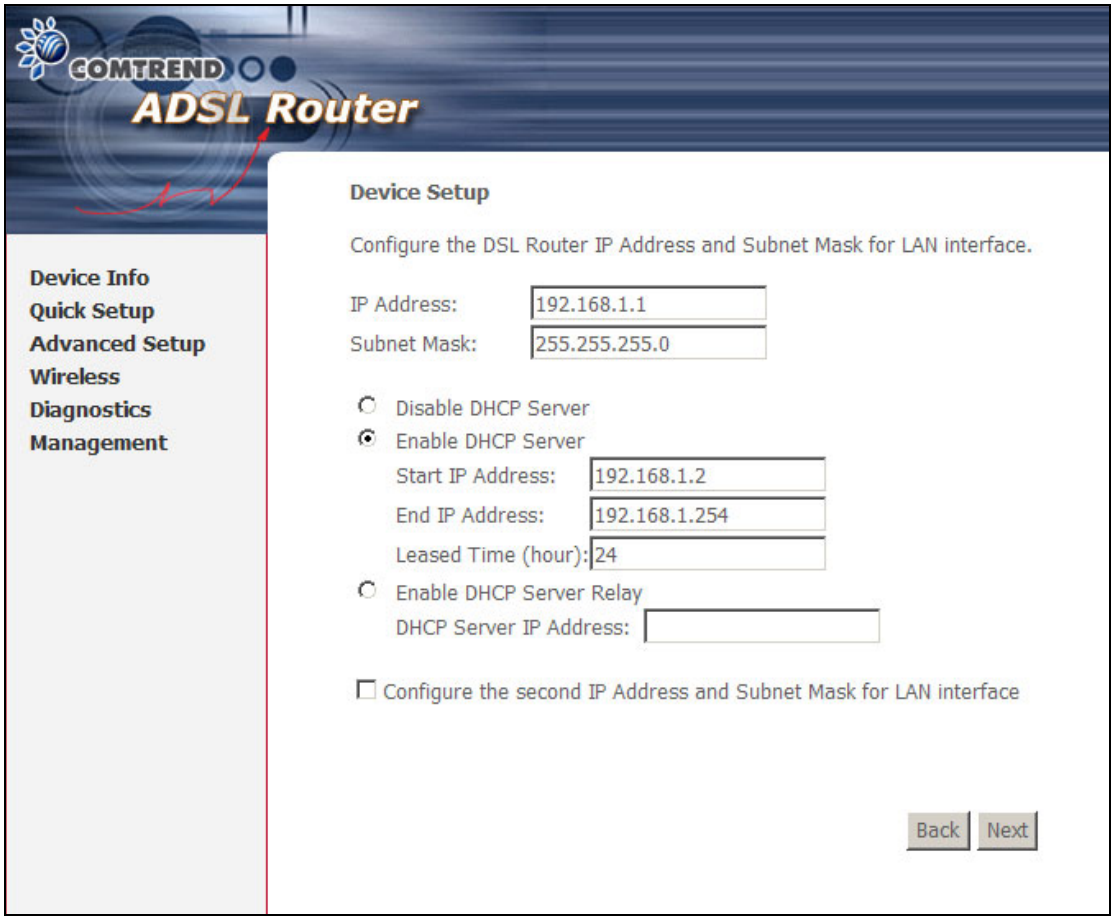


Enable IGMP Multicast
Tick the checkbox ☑ to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers.

Enable WAN Service
Tick the checkbox ☑ to enable the WAN service.

Service Name: This is the WAN Service label.

STEP 6: Upon completion, click **Next**. The following screen appears.



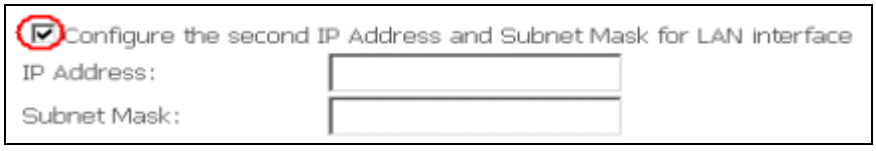
This screen allows for the configuration of the CT-5361T LAN interface IP address, subnet mask and DHCP server. To auto-assign IP addresses, DNS server and default gateway to other LAN devices, select the **Enable DHCP server** radio box. You must also enter the start and end IP address and DHCP leased time.

NOTE:	LAN interfaces (e.g. USB and Ethernet) share the same subnet since they are bridged within the router.

Select **Enable DHCP Server Relay** (if required), and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets to the remote DHCP server. The remote DHCP server will provide the IP address.

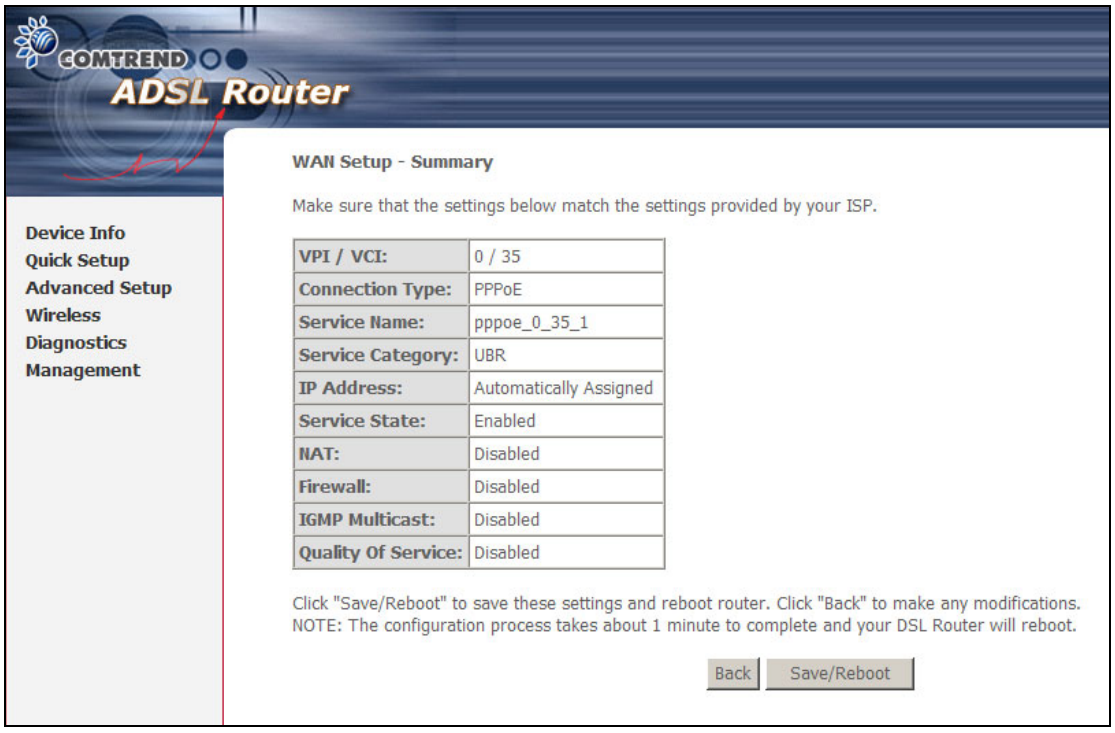
NOTE:	**Enable DHCP Server Relay** will not display if NAT is enabled.

To configure a secondary IP address for the LAN port, click the checkbox ☑ shown.



STEP 7: Click **Next** to proceed to the Wireless Setup screen. To enable wireless, tick the checkbox ☑ and click **Next**. If you wish to do so, you may also change the SSID (Service Set Identifier) at this point.

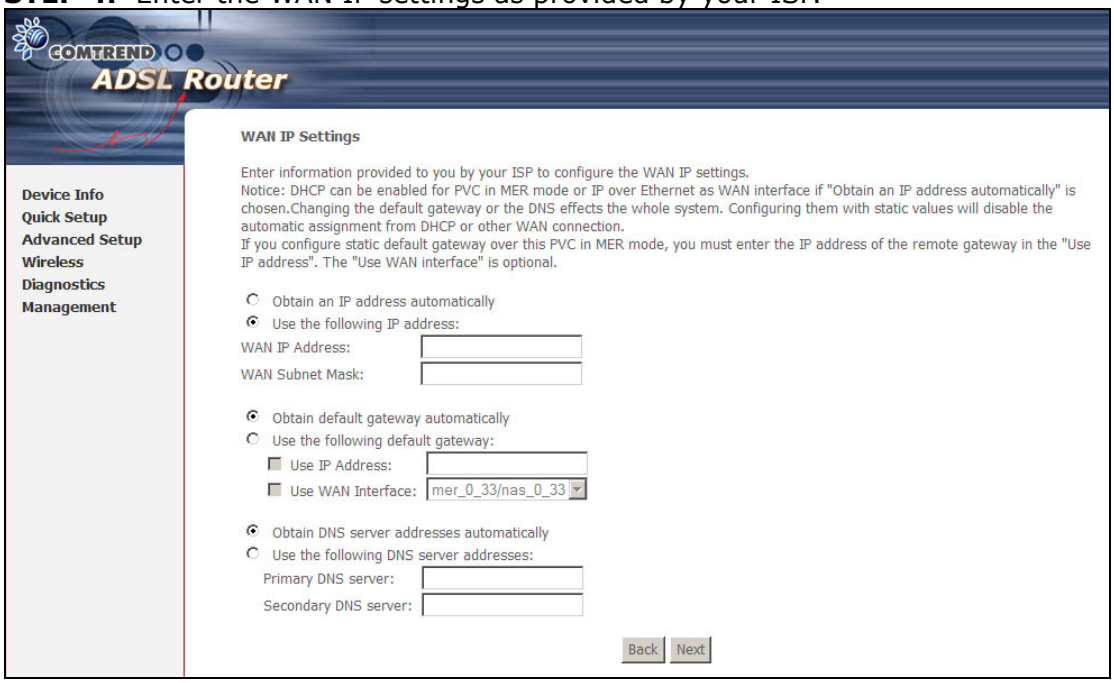
STEP 8: Click **Next** to display the configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.


COMTREND
ADSL Router
Device Info
Quick Setup
Advanced Setup
Wireless
Diagnostics
Management
WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
VPI / VCI: 0 / 35
Connection Type: PPPoE
Service Name: pppoe_0_35_1
Service Category: UBR
IP Address: Automatically Assigned
Service State: Enabled
NAT: Disabled
Firewall: Disabled
IGMP Multicast: Disabled
Quality Of Service: Disabled
Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.
Back
Save/Reboot

After clicking **Save/Reboot**, the router will save the configuration to the flash memory and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info screen automatically. The CT-5361T is ready for operation when the front panel LED indicators display as described in section 2.4 LED Indicators.

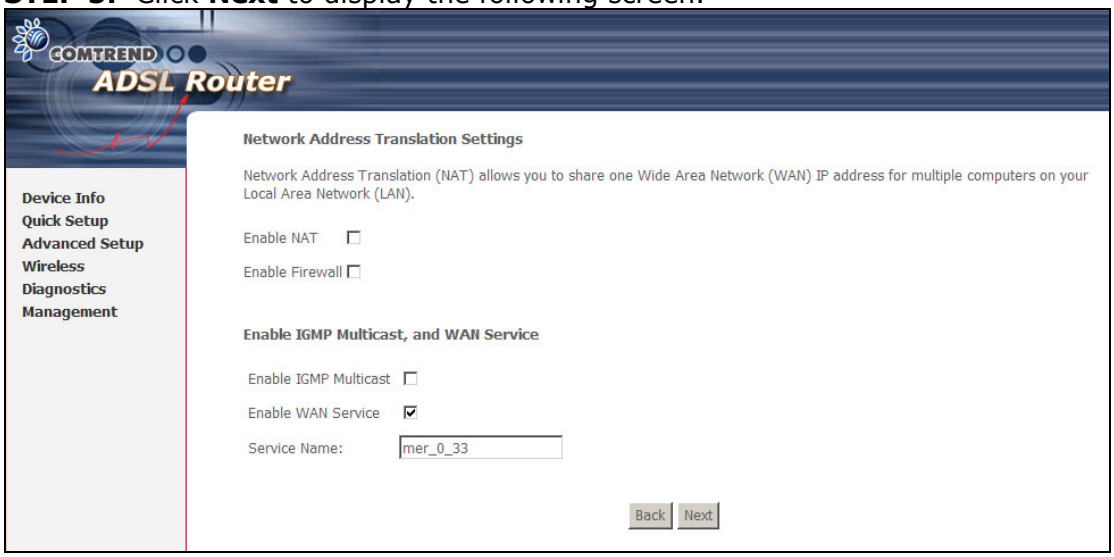
4.2.2 MAC Encapsulation Routing (MER)

STEP 4: Enter the WAN IP settings as provided by your ISP.


COMTREND
ADSL Router
Device Info
Quick Setup
Advanced Setup
Wireless
Diagnostics
Management
WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: DHCP can be enabled for PVC in MER mode or IP over Ethernet as WAN interface if "Obtain an IP address automatically" is chosen.Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.
If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional.
Obtain an IP address automatically
Use the following IP address:
WAN IP Address:
WAN Subnet Mask:
Obtain default gateway automatically
Use the following default gateway:
Use IP Address:
Use WAN Interface:
mer_0_33/nas_0_33
Obtain DNS server addresses automatically
Use the following DNS server addresses:
Primary DNS server:
Secondary DNS server:
Back
Next

DHCP can be enabled if the **Obtain an IP address automatically** checkbox ☑ is checked. Configuring the default gateway or the DNS with static values will disable the automatic assignment from DHCP or other WAN connection.

STEP 5: Click **Next** to display the following screen.



Enable NAT
If the LAN is configured with a private IP address, the user should select this checkbox ☑. The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox ☑ should not be selected, so as to free up system resources for improved performance.

Enable Firewall
If this checkbox ☑ is selected, the Security submenu will be displayed on the

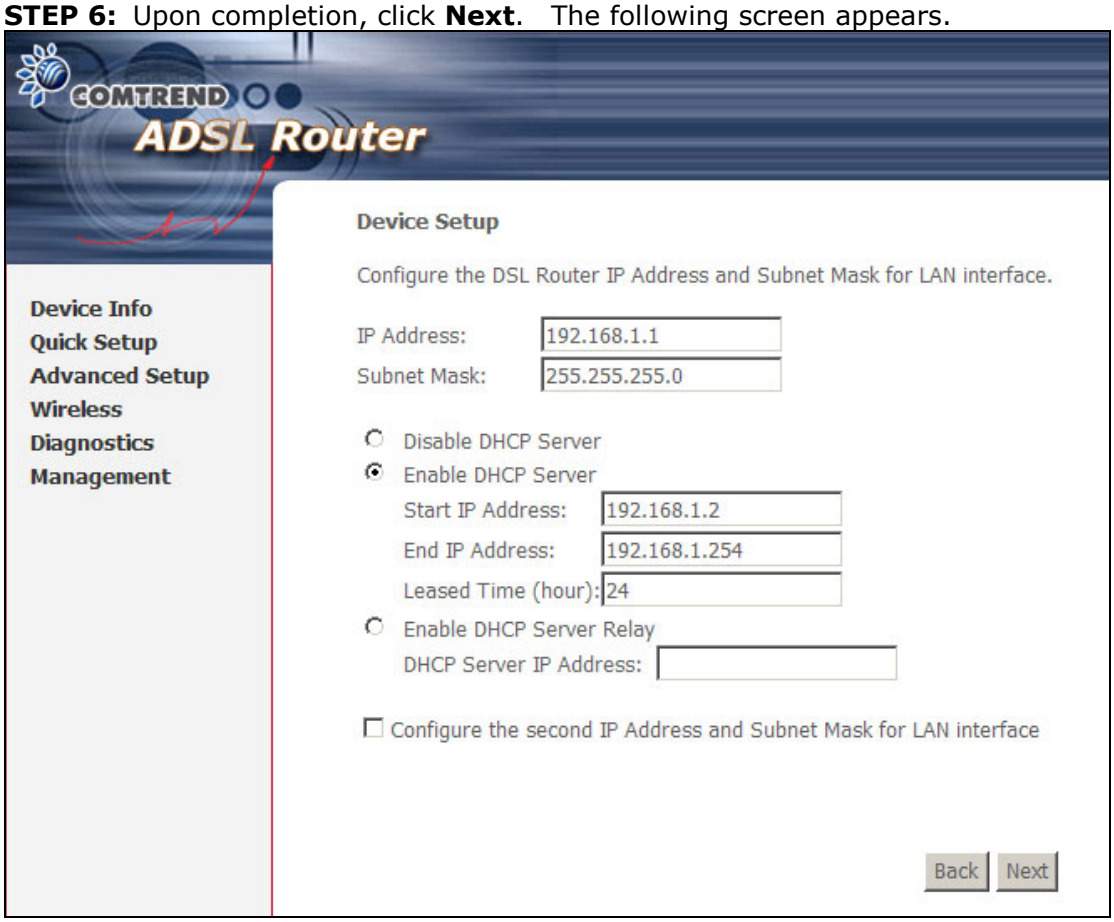
Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should be de-selected to free up system resources for better performance.

Enable IGMP Multicast
Tick the checkbox ☑ to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers.

Enable WAN Service
Tick the checkbox ☑ to enable the WAN service.

Service Name is user-defined.

STEP 6: Upon completion, click **Next**. The following screen appears.



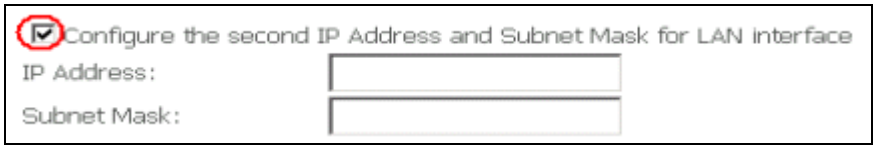
This screen allows for the configuration of the CT-5361T LAN interface IP address, subnet mask and DHCP server. To auto-assign IP addresses, DNS server and default gateway to LAN devices, select the **Enable DHCP server** radio box. You must also enter the start and end IP address and DHCP leased time.

NOTE:	LAN interfaces (e.g. USB and Ethernet) share the same subnet since they are bridged within the router.

Select **Enable DHCP Server Relay** (if required), and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets to the remote DHCP server. The remote DHCP server will provide the IP address.

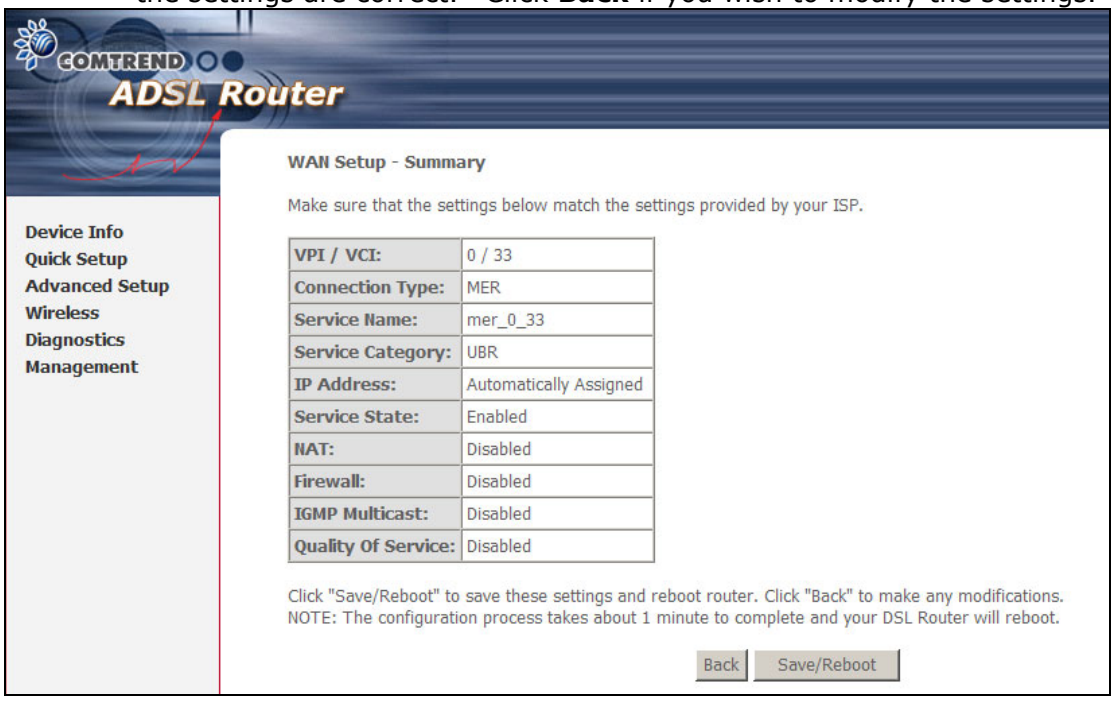
NOTE:	The **Enable DHCP Server Relay** option will not display if NAT is enabled.

To configure a secondary IP address for the LAN port, click the checkbox ☑ shown.



STEP 7: Click **Next** to proceed to the Wireless Setup screen. To enable wireless, tick the checkbox ☑ and click **Next**. If you wish to do so, you may also change the SSID (Service Set Identifier) at this point.

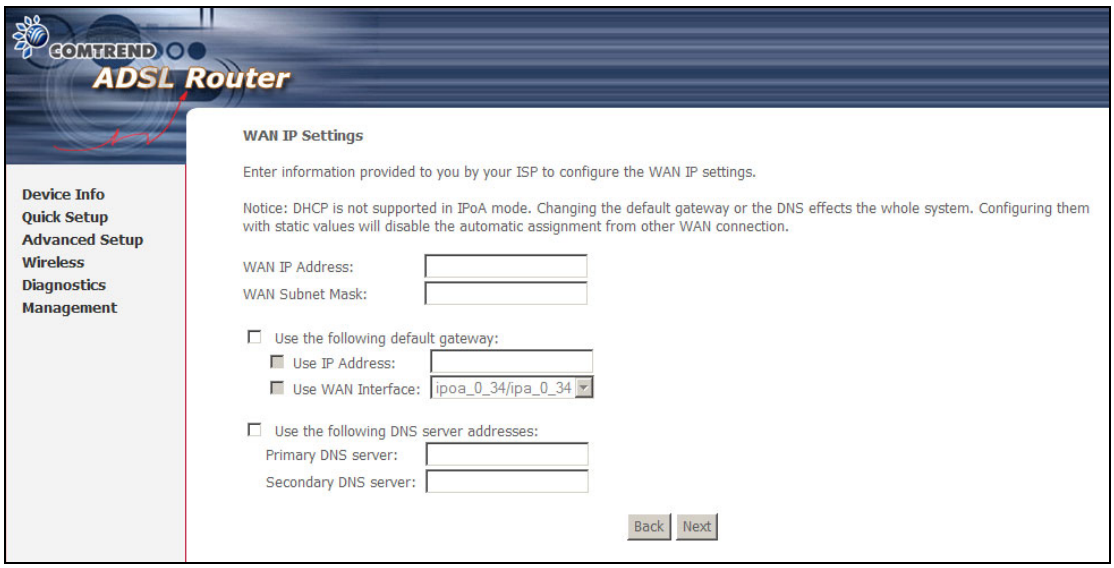
STEP 8: Click **Next** to display the configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.


COMTREND
ADSL Router
Device Info
Quick Setup
Advanced Setup
Wireless
Diagnostics
Management
WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
VPI / VCI: 0 / 33
Connection Type: MER
Service Name: mer_0_33
Service Category: UBR
IP Address: Automatically Assigned
Service State: Enabled
NAT: Disabled
Firewall: Disabled
IGMP Multicast: Disabled
Quality Of Service: Disabled
Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.
Back
Save/Reboot

After clicking **Save/Reboot**, the router will save the configuration to the flash memory and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info screen automatically. The CT-5361T is ready for operation when the front panel LED indicators display as described in section 2.4 LED Indicators.

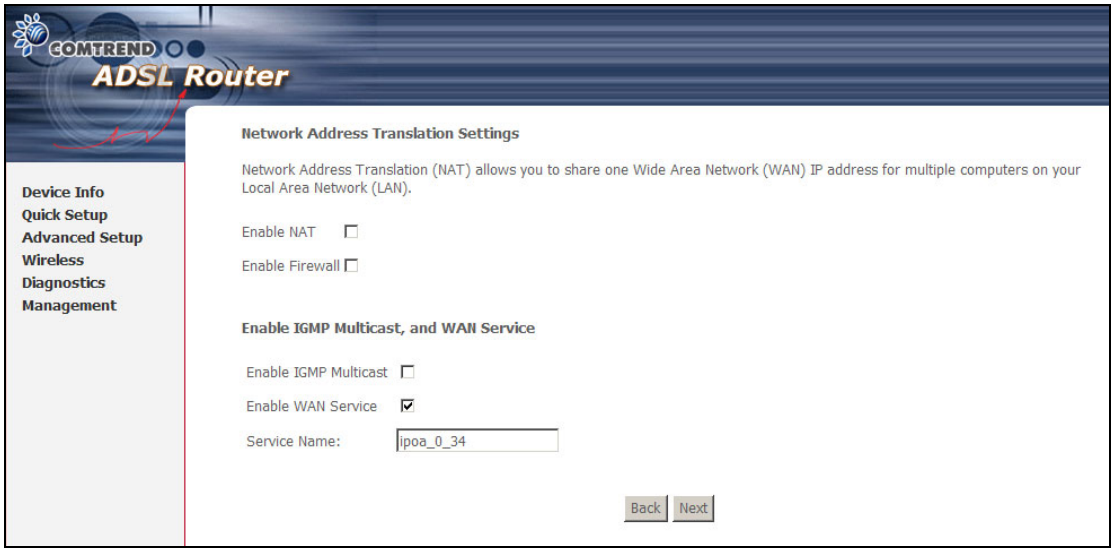
4.2.3 IP Over ATM

STEP 4: Enter the WAN IP settings as provided by your ISP.


COMTREND
ADSL Router
Device Info
Quick Setup
Advanced Setup
Wireless
Diagnostics
Management
WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: DHCP is not supported in IPoA mode. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from other WAN connection.
WAN IP Address:
WAN Subnet Mask:
Use the following default gateway:
Use IP Address:
Use WAN Interface:
ipoa_0_34/ipa_0_34
Use the following DNS server addresses:
Primary DNS server:
Secondary DNS server:
Back
Next

Since DHCP is not supported over IPoA, the default gateway settings and DNS server addresses must be entered here. These should be provided by your ISP.

STEP 5: Click **Next** to display the following screen.



Enable NAT
If the LAN is configured with a private IP address, the user should select this checkbox ☑. The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox ☑ should not be selected, so as to free up system resources for improved performance.

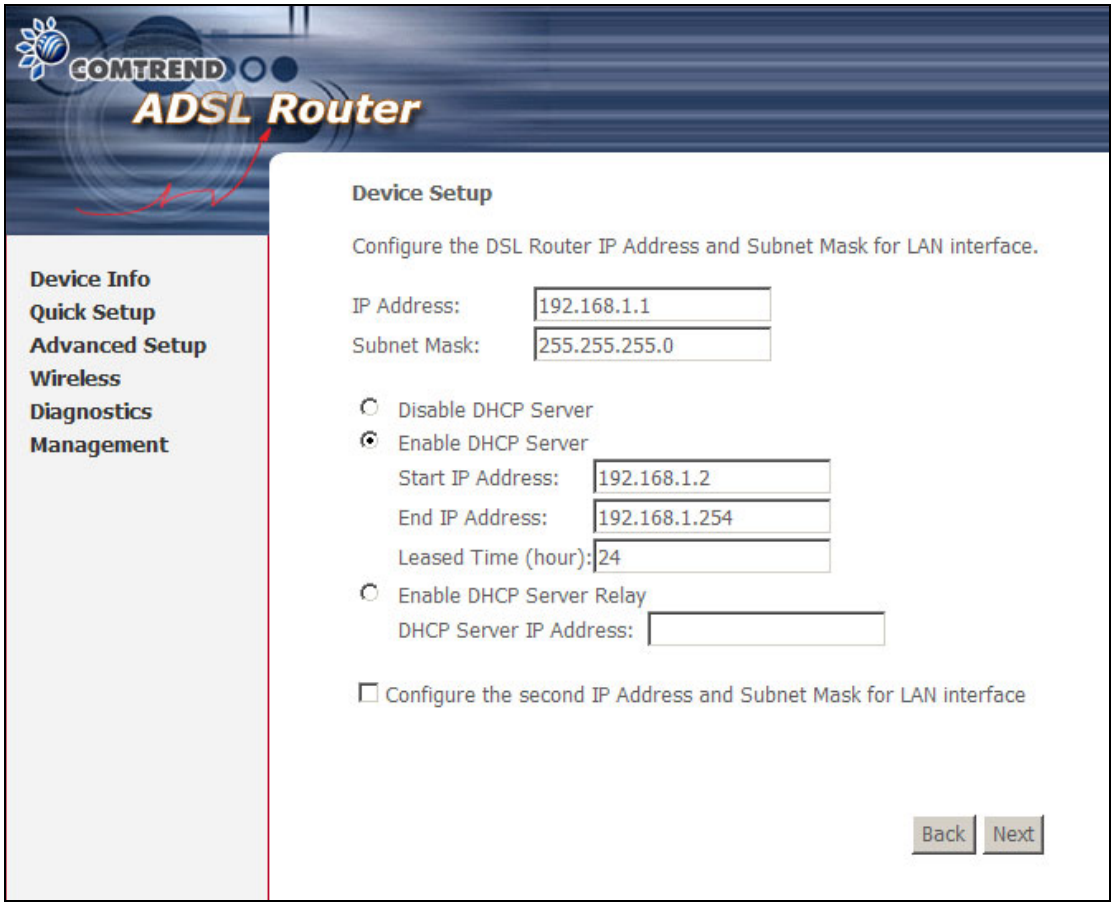
Enable Firewall
If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should be de-selected to free up system resources for better performance.

Enable IGMP Multicast
Tick the checkbox ☑ to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers.

Enable WAN Service
Tick the checkbox ☑ to enable the WAN service.

Service Name is user-defined.

STEP 6: Upon completion, click **Next**. The following screen appears.



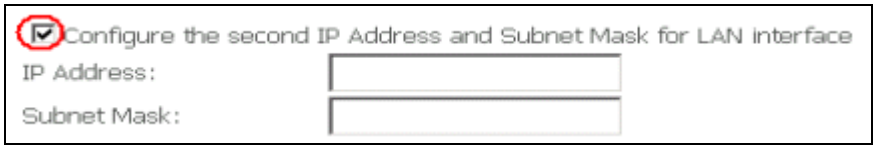
This screen allows for the configuration of the CT-5361T LAN interface IP address, subnet mask and DHCP server. To auto-assign IP addresses, DNS server and default gateway to LAN devices, select the **Enable DHCP server** radio box. You must also enter the start and end IP address and DHCP leased time.

NOTE:	LAN interfaces (e.g. USB and Ethernet) share the same subnet since they are bridged within the router.

Select **Enable DHCP Server Relay** (if required), and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets to the remote DHCP server. The remote DHCP server will provide the IP address.

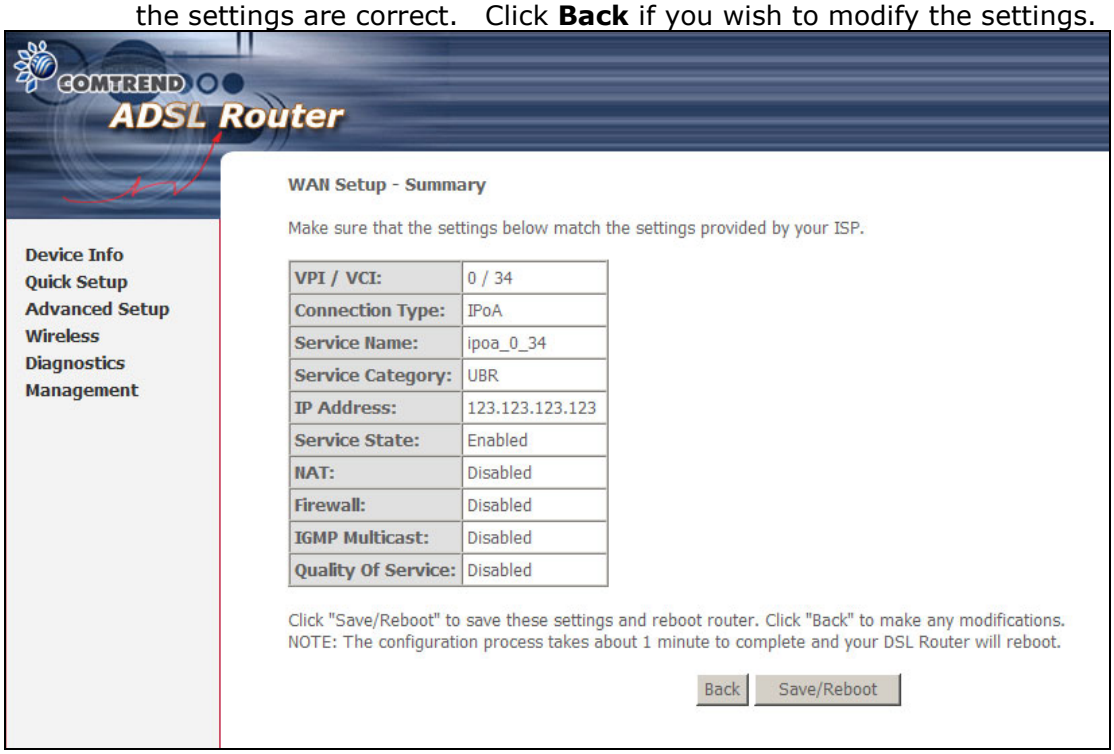
NOTE:	The **Enable DHCP Server Relay** option will not display if NAT is enabled.

To configure a secondary IP address for the LAN port, click the checkbox ☑ shown.



STEP 7: Click **Next** to proceed to the Wireless Setup screen. To enable wireless, tick the checkbox ☑ and click **Next**. If you wish to do so, you may also change the SSID (Service Set Identifier) at this point.

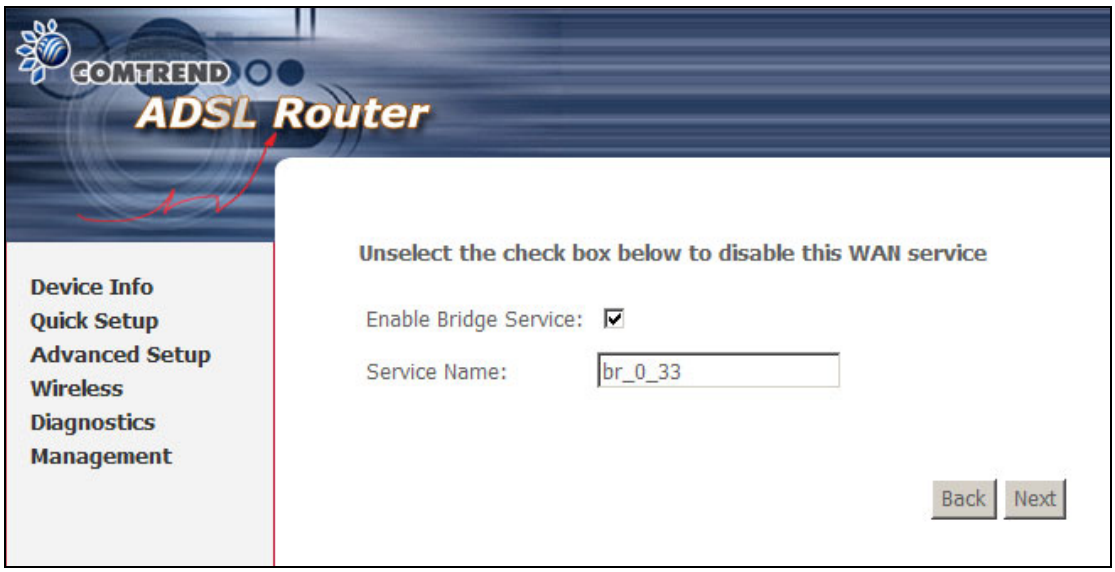
STEP 8: Click **Next** to display the configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.



After clicking **Save/Reboot**, the router will save the configuration to the flash memory and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info screen automatically. The CT-5361T is ready for operation when the front panel LED indicators display as described in section 2.4 LED Indicators.

4.2.4 Bridging

STEP 4: To enable bridge service, tick the checkbox ☑ and enter a service name.

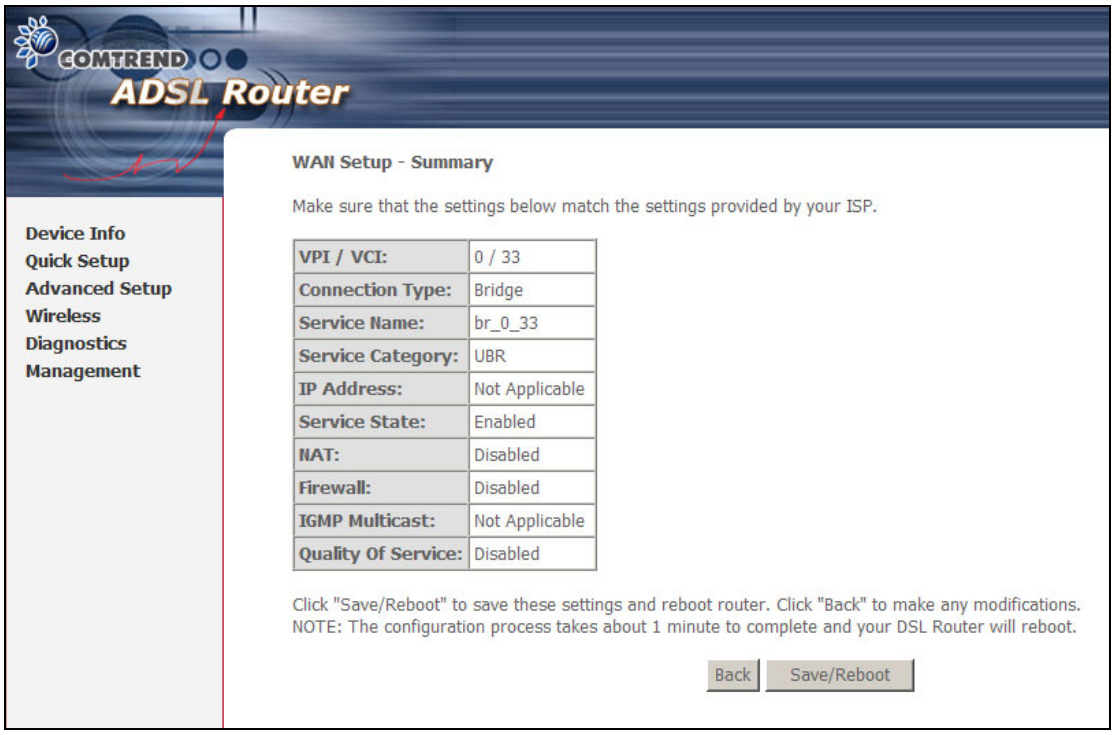


STEP 5: Click **Next** to display the following screen.

Enter the IP address and subnet mask for the LAN interface. These settings are used to manage the CT-5361T. In bridge mode, there is no WAN IP address and therefore no remote access to the router for technical support or other purposes.

STEP 6: Click **Next** to proceed to the Wireless Setup screen. To enable wireless, tick the checkbox ☑ and click **Next**. If you wish to do so, you may also change the SSID (Service Set Identifier) at this point.

STEP 7: Click **Next** to display the configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.


COMTREND
ADSL Router
WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
VPI / VCI: 0 / 33
Connection Type: Bridge
Service Name: br_0_33
Service Category: UBR
IP Address: Not Applicable
Service State: Enabled
NAT: Disabled
Firewall: Disabled
IGMP Multicast: Not Applicable
Quality Of Service: Disabled
Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.
Back
Save/Reboot
Device Info
Quick Setup
Advanced Setup
Wireless
Diagnostics
Management

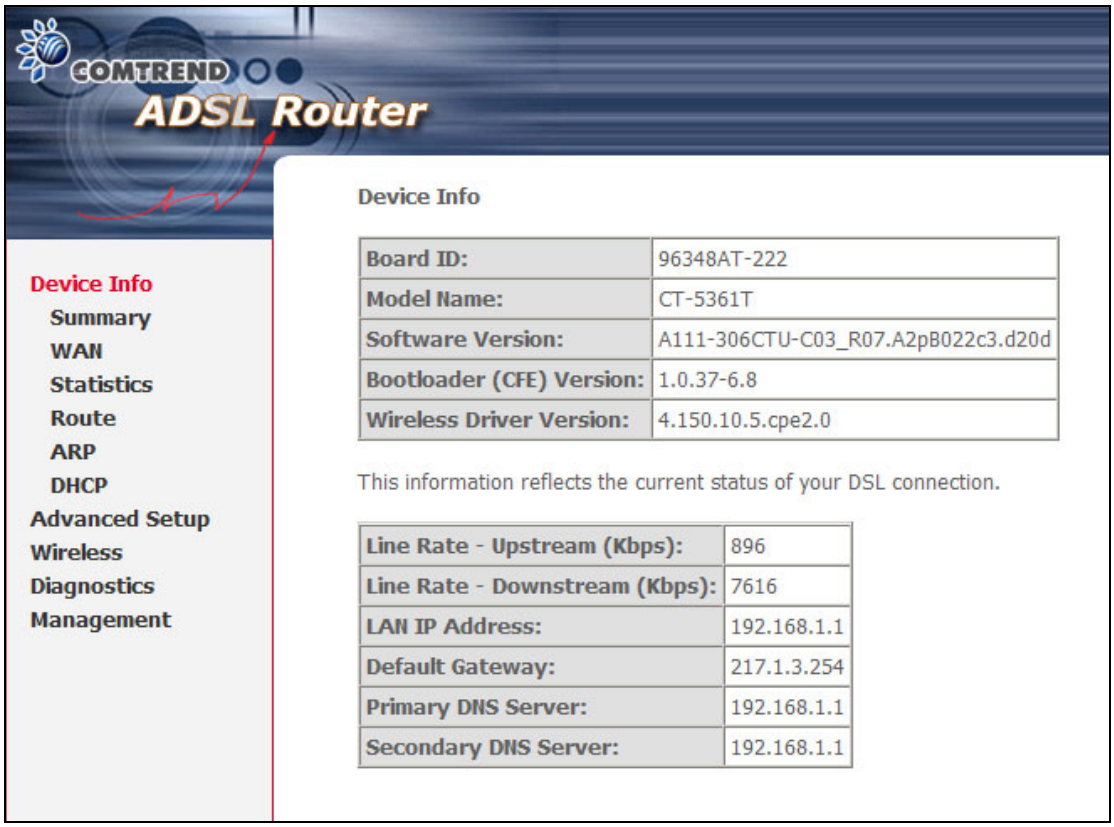
After clicking **Save/Reboot**, the router will save the configuration to the flash memory and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info screen automatically. The CT-5361T is ready for operation when the front panel LED indicators display as described in section 2.4 LED Indicators.

Chapter 5 Device Information

The web user interface is divided into two windowpanes, the main menu (at left) and the display screen (on the right). The main menu has the several options and selecting each of these options opens a submenu with more selections.

NOTE:	The menu items shown are based upon the configured connection and user account privileges. For example, in the Advanced Setup menu, if NAT and Firewall are enabled, the main menu will display the NAT and Security submenus. If either is disabled, their corresponding menu(s) will also be disabled.

Device Info is the first selection on the main menu so it will be discussed first. Subsequent chapters will introduce the other main menu options in sequence.

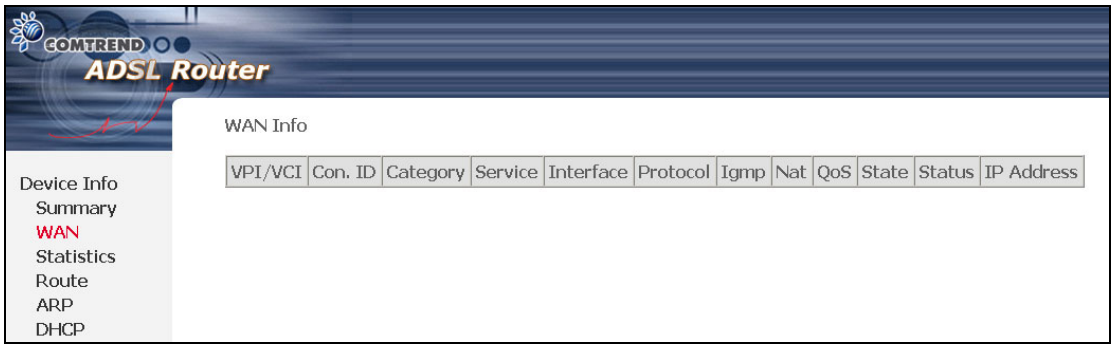


The Device Info Summary screen (shown above) is the default startup screen.

It provides summary information regarding hardware, software, data transmission (line rates), and the IP configuration of the device.

5.1 WAN

Select **WAN** from the Device Info submenu to display the configured PVC(s).



Heading	Description
VPI/VCI	ATM VPI (0-255) / VCI (32-65535)
Con. ID	WAN connection ID number
Category	ATM service category
Service	Name of the WAN connection
Interface	Name of the interface for WAN
Protocol	Shows the connection type
IGMP	Shows Internet Group Management Protocol (IGMP) status
Nat	Shows Network Address Translation (NAT) status
QoS	Shows Quality of Service (QoS) status
State	Shows the connection state of the WAN connection
Status	Lists the status of DSL link
IP Address	Shows WAN IP address

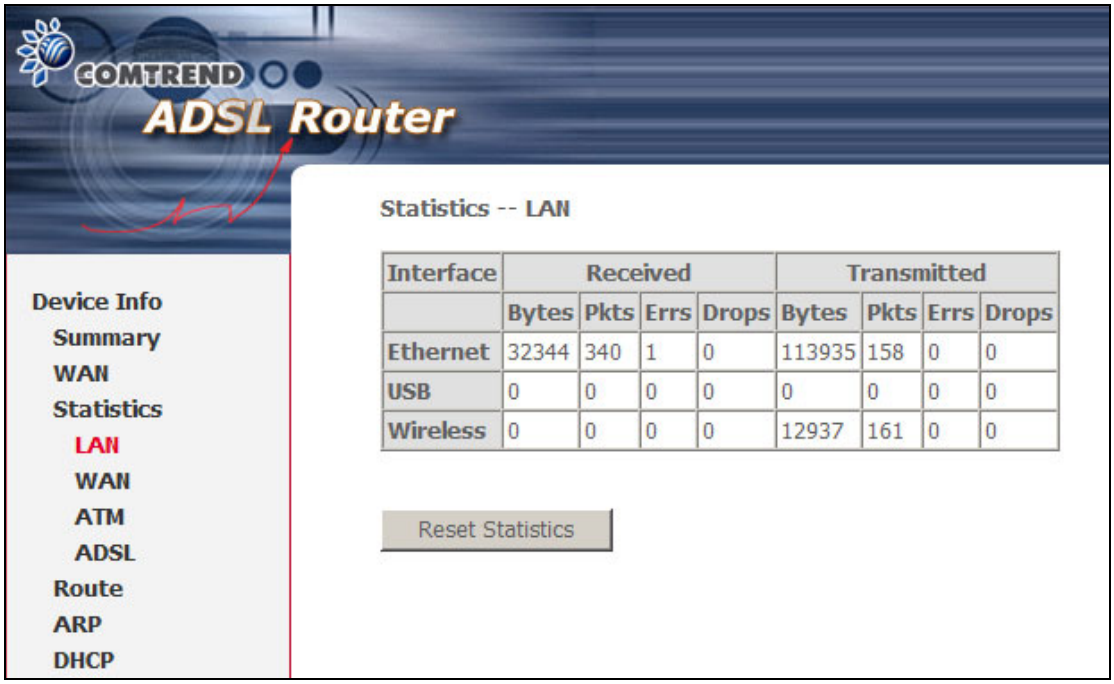
5.2 Statistics

This selection provides LAN, WAN, ATM and ADSL statistics.

NOTE:	These screens are updated every 15 seconds.

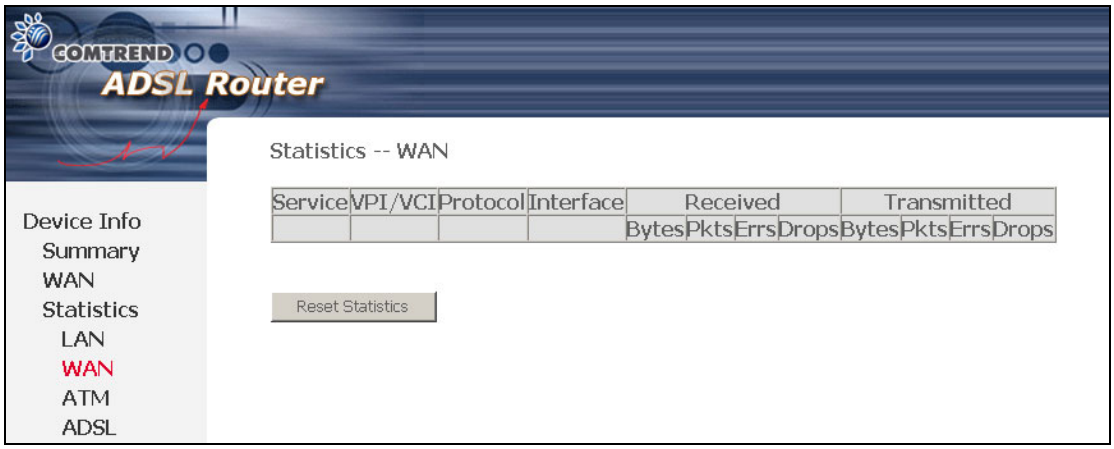
5.2.1 LAN Statistics

This screen shows data traffic statistics for each LAN interface.



Heading	Description
Interface	LAN interfaces
Received/Transmitted: - Bytes - Pkts - Errs - Drops	Number of Bytes Number of Packets Number of packets with errors Number of dropped packets

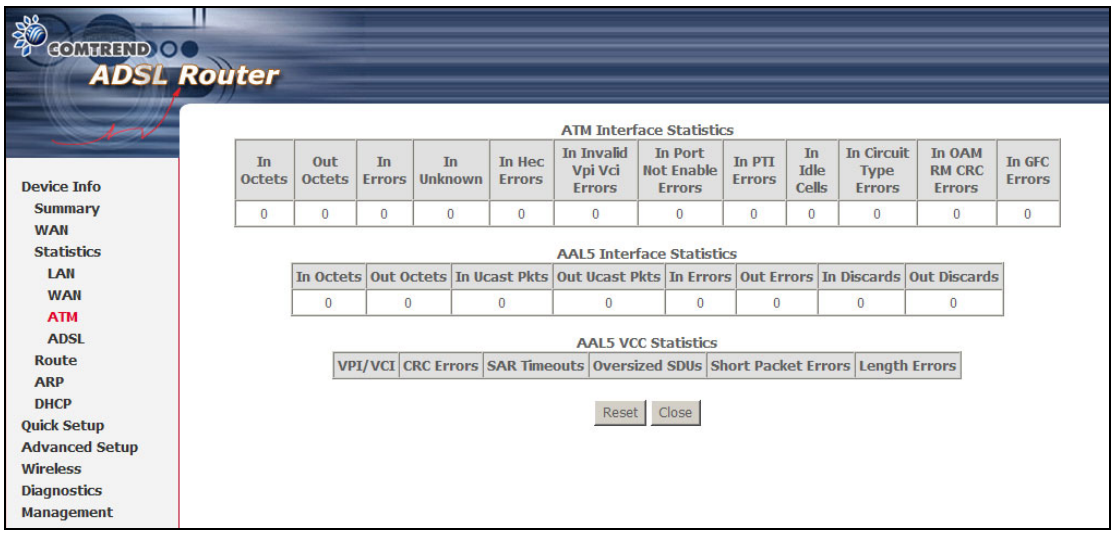
5.2.2 WAN Statistics



Heading	Description
Service	WAN service label
VPI/VCI	ATM Virtual Path/Channel Identifiers
Protocol	Connection type (e.g. PPPoE, IPoA, Bridge)
Interface	Shows connection interfaces
Received/Transmitted - Bytes - Pkts - Errs - Drops	Number of Bytes Number of Packets Number of packets with errors Number of dropped packets

5.2.3 ATM statistics

The following figure shows the ATM statistics screen.



ATM Interface Statistics

Heading	Description
In Octets	Number of received octets over the interface
Out Octets	Number of transmitted octets over the interface
In Errors	Number of cells dropped due to uncorrectable HEC errors
In Unknown	Number of received cells discarded during cell header validation, including cells with unrecognized VPI/VCI values, and cells with invalid cell header patterns. If cells with undefined PTI values are discarded, they are also counted here.
In Hec Errors	Number of cells received with an ATM Cell Header HEC error
In Invalid Vpi Vci Errors	Number of cells received with an unregistered VCC address.
In Port Not Enable Errors	Number of cells received on a port that has not been enabled.
In PTI Errors	Number of cells received with an ATM header Payload Type Indicator (PTI) error
In Idle Cells	Number of idle cells received
In Circuit Type Errors	Number of cells received with an illegal circuit type
In OAM RM CRC Errors	Number of OAM and RM cells received with CRC errors
In GFC Errors	Number of cells received with a non-zero GFC.

AAL5 Interface Statistics

Heading	Description
In Octets	Number of received AAL5/AAL0 CPCS PDU octets
Out Octets	Number of received AAL5/AAL0 CPCS PDU octets transmitted
In Ucast Pkts	Number of received AAL5/AAL0 CPCS PDUs passed to a higher-layer for transmission
Out Ucast Pkts	Number of received AAL5/AAL0 CPCS PDUs received from a higher layer for transmission

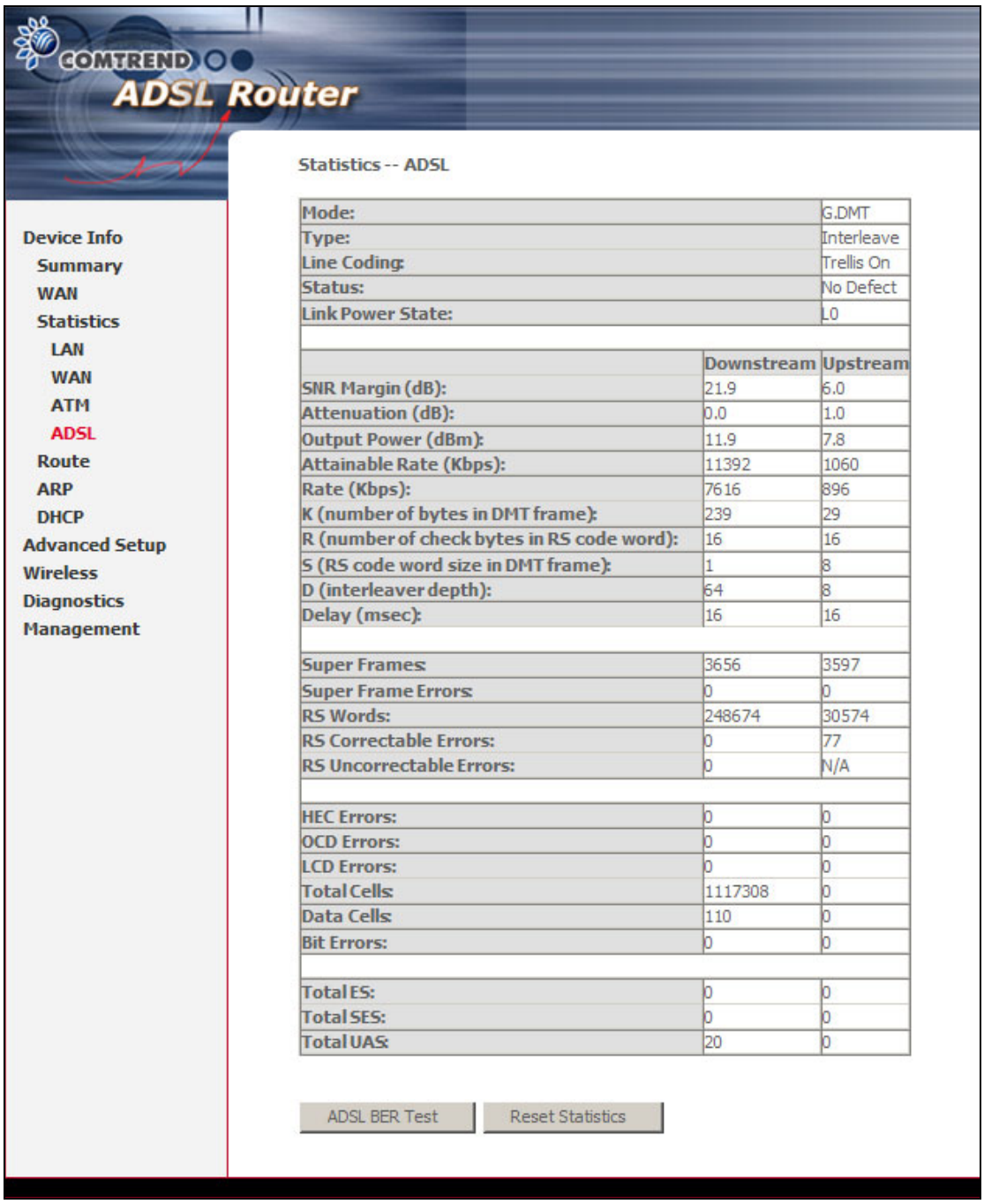
In Errors	Number of received AAL5/AAL0 CPCS PDUs received that contain an error. These errors include CRC-32 errors.
Out Errors	Number of received AAL5/AAL0 CPCS PDUs that could not be transmitted due to errors.
In Discards	Number of received AAL5/AAL0 CPCS PDUs discarded due to an input buffer overflow condition.
Out Discards	This field is not currently used

AAL5 VCC Statistics

Heading	Description
VPI/VCI	ATM Virtual Path/Channel Identifiers
CRC Errors	Number of PDUs received with CRC-32 errors
SAR TimeOuts	Number of partially re-assembled PDUs that were discarded because they were not fully re-assembled within the required period of time. If the re-assembly time is not supported, then this object contains a zero value.
Oversized SDUs	Number of PDUs discarded because the corresponding SDU was too large
Short Packet Errors	Number of PDUs discarded because the PDU length was less than the size of the AAL5 trailer
Length Errors	Number of PDUs discarded because the PDU length did not match the length in the AAL5 trailer

5.2.4 ADSL Statistics

The following figure shows the ADSL Statistics screen in G.Dmt mode.



Click the **Reset Statistics** button to refresh this screen.

Field	Description
Mode	G.Dmt, G.lite, T1.413, ADSL2, ADSL2+
Type	Channel type Interleave or Fast
Line Coding	Trellis On/Off
Status	Lists the status of the DSL link
Link Power State	Link output power state.

SNR Margin (dB)	Signal to Noise Ratio (SNR) margin
Attenuation (dB)	Estimate of average loop attenuation in the downstream direction.
Output Power (dBm)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain.
Rate (Kbps)	Current sync rate.

In G.DMT mode, the following section is inserted.

K	Number of bytes in DMT frame
R	Number of check bytes in RS code word
S	RS code word size in DMT frame
D	The interleaver depth
Delay	The delay in milliseconds (msec)

In ADSL2+ mode, the following section is inserted.

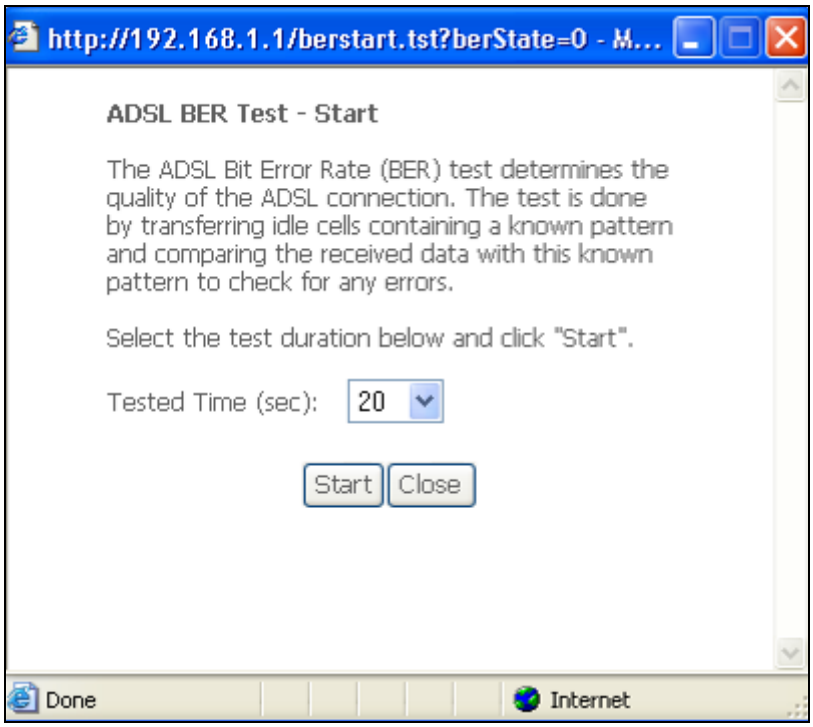
MSGc	Number of bytes in overhead channel message
B	Number of bytes in Mux Data Frame
M	Number of Mux Data Frames in FEC Data Frame
T	Max Data Frames over sync bytes
R	Number of check bytes in FEC Data Frame
S	Ratio of FEC over PMD Data Frame length
L	Number of bits in PMD Data Frame
D	The interleaver depth
Delay	The delay in milliseconds (msec)

Super Frames	Total number of super frames
Super Frame Errors	Number of super frames received with errors
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors

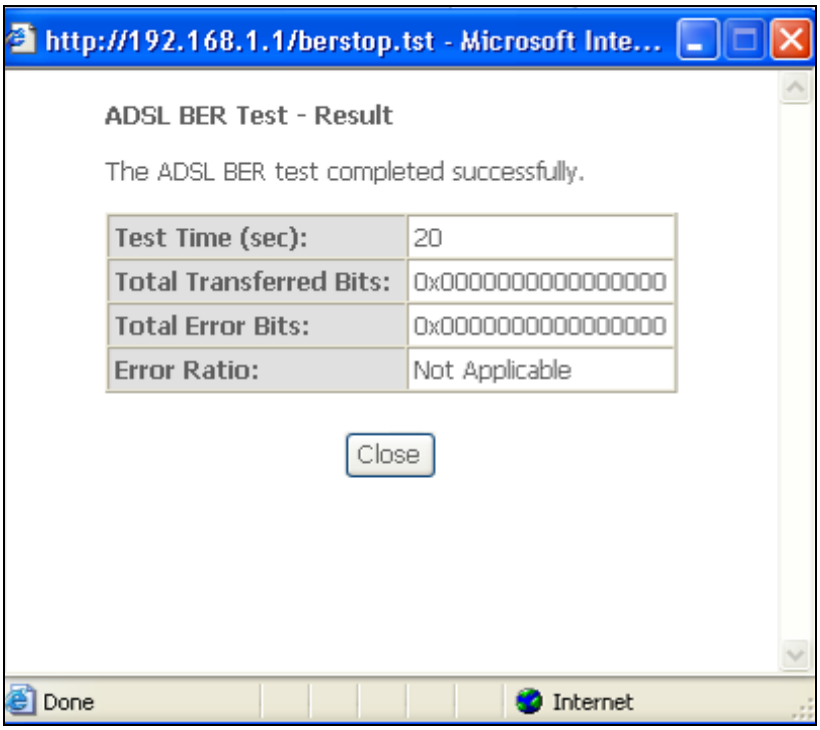
HEC Errors	Total Number of Header Error Checksum errors
OCD Errors	Total Number of out-of-cell Delineation errors
LCD Errors	Total number of Loss of Cell Delineation
Total Cells	Total number of ATM cells (including idle + data cells)
Data Cells	Total number of ATM data cells
Bit Errors	Total number of bit errors

Total ES	Total Number of Errored Seconds
Total SES	Total Number of Severely Errored Seconds
Total UAS	Total Number of Unavailable Seconds

Within the ADSL Statistics window, a Bit Error Rate (BER) test can be started using the **ADSL BER Test** button. A small window will open when the button is pressed; it will appear as shown below. Click **Start** to start the test or **Close**.

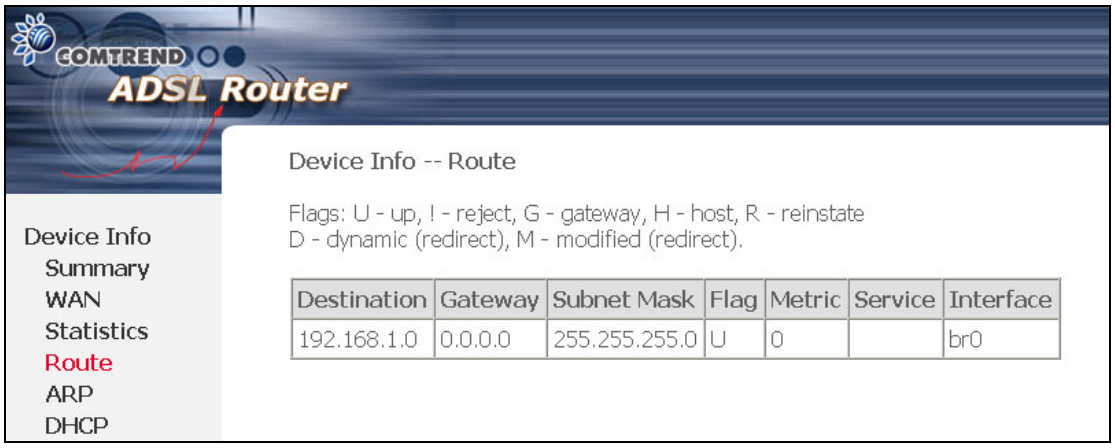

http://192.168.1.1/berstart.tst?berState=0 - M...
ADSL BER Test - Start
The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.
Select the test duration below and click "Start".
Tested Time (sec): 20
Start
Close
Done
Internet

If the test is successful, the pop-up window will display as follows.



5.3 Route

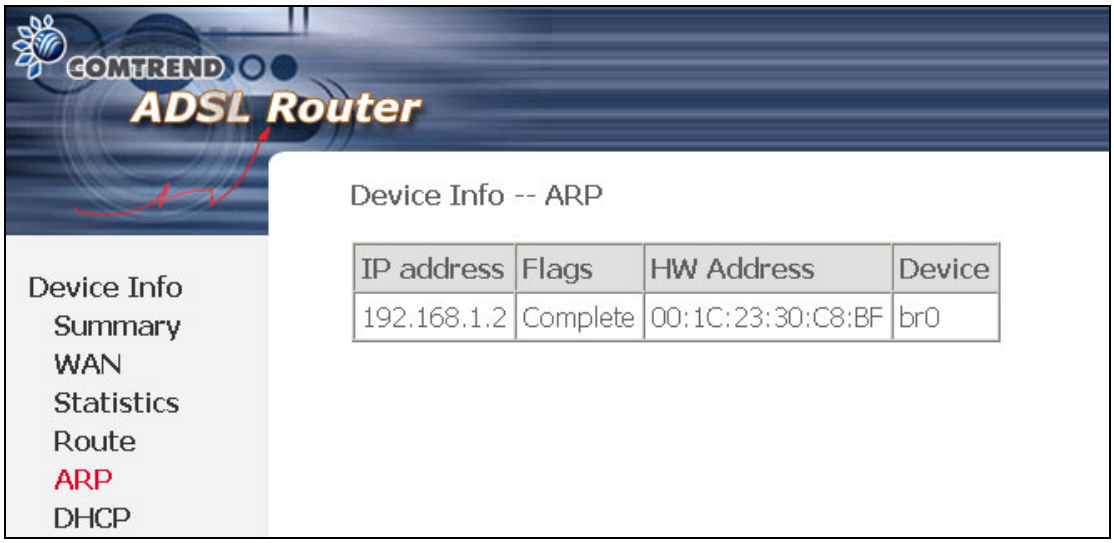
Choose **Route** to display the routes that the CT-5361T has found.



Field	Description
Destination	Destination network or destination host
Gateway	Next hub IP address
Subnet Mask	Subnet Mask of Destination
Flag	U: route is up !: reject route G: use gateway H: target is a host R: reinstate route for dynamic routing D: dynamically installed by daemon or redirect M: modified from routing daemon or redirect
Metric	The 'distance' to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.
Service	Shows the name for WAN connection
Interface	Shows connection interfaces

5.4 ARP

Click **ARP** to display the ARP information.



Field	Description
IP address	Shows IP address of host pc
Flags	Complete, Incomplete, Permanent, or Publish
HW Address	Shows the MAC address of host pc
Device	Shows the connection interface

5.5 DHCP

Click **DHCP** to display all DHCP Leases.

Field	Description
Hostname	Shows the device/host/PC network name
MAC Address	Shows the Ethernet MAC address of the device/host/PC
IP address	Shows IP address of device/host/PC
Expires In	Shows how much time is left for each DHCP Lease

Chapter 6 Advanced Setup

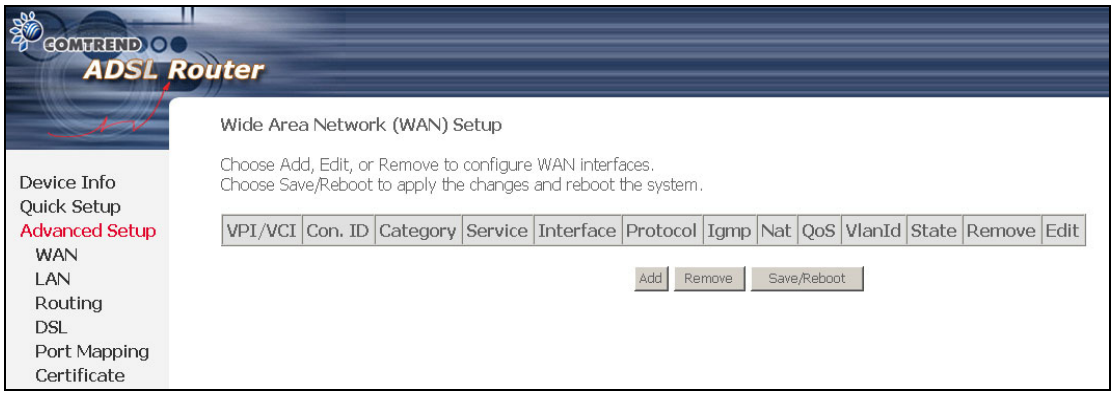
This chapter explains the following screens:

6.1 WAN	6.6 Routing
6.2 LAN	6.7 DNS
6.3 NAT	6.8 DSL
6.4 Security	6.9 Port Mapping
6.5 Quality of Service	6.10 Certificate

6.1 WAN

This screen allows for the configuration of WAN interfaces.

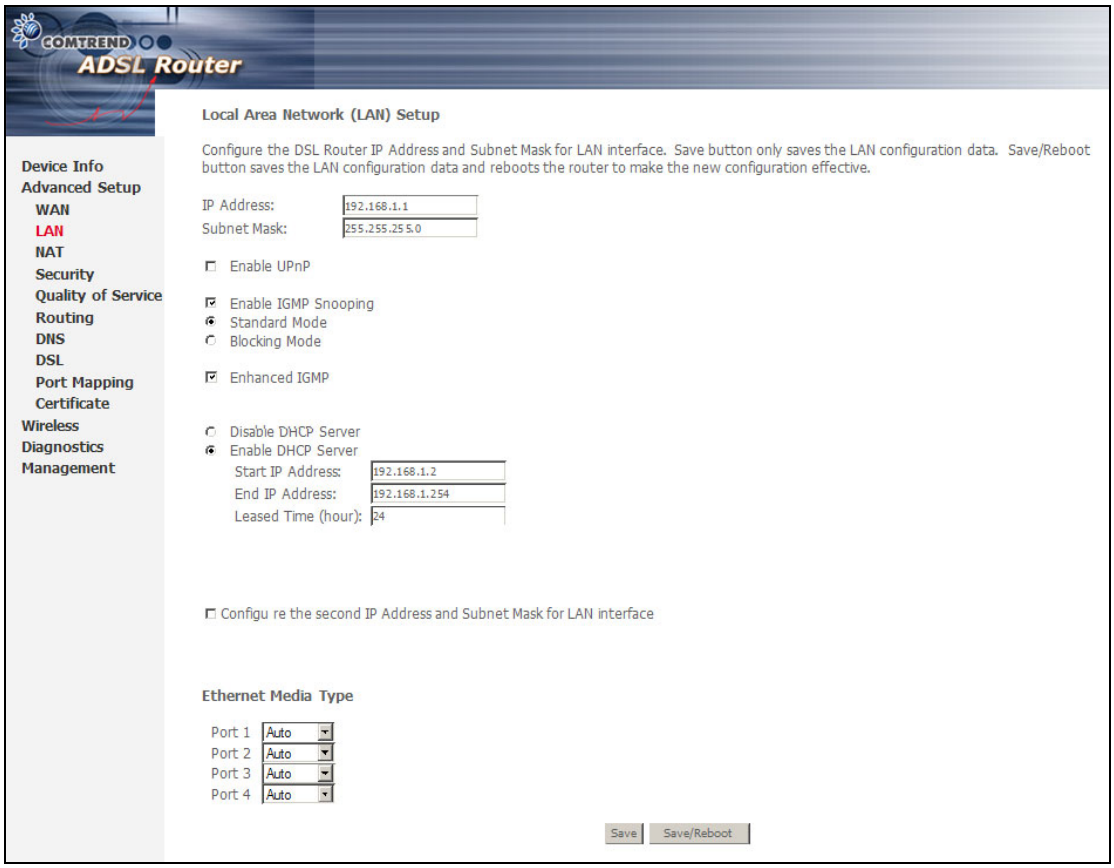
To **Add** a new WAN connection, click the **Add** button. To edit an existing connection, click the **Edit** button next to the connection. To complete the **Add** or **Edit** go to **STEP 2** in section 4.2 Manual Quick Setup. To remove a connection select its radio button under the **Remove** column of the table and click the **Remove** button under the table.



Heading	Description
VPI/VCI	ATM VPI (0-255) / VCI (32-65535)
Con. ID	WAN connection ID number
Category	ATM service category
Service	Name of the WAN connection
Interface	Name of the interface for WAN
Protocol	Shows the connection type
Igmp	Shows Internet Group Management Protocol (IGMP) status
Nat	Shows Network Address Translation (NAT) status
QoS	Shows Quality of Service (QoS) status
VlanId	VLAN ID is used for VLAN Tagging (IEEE 802.1Q)
State	Shows the connection state of the WAN connection
Remove	Used to select connections for removal
Edit	Used to edit connections

6.2 LAN

From this screen, LAN interface settings can be configured.



NOTE: NAT is enabled so **UPnP** is shown above (see underlined notes below).

Consult the field descriptions below for more details.

IP Address: Enter the IP address for the LAN port.

Subnet Mask: Enter the subnet mask for the LAN port.

Enable UPnP: Tick the box to enable Universal Plug and Play.
This option is hidden when NAT disabled or if no PVC exists

Enable IGMP Snooping: Enable by ticking the box.

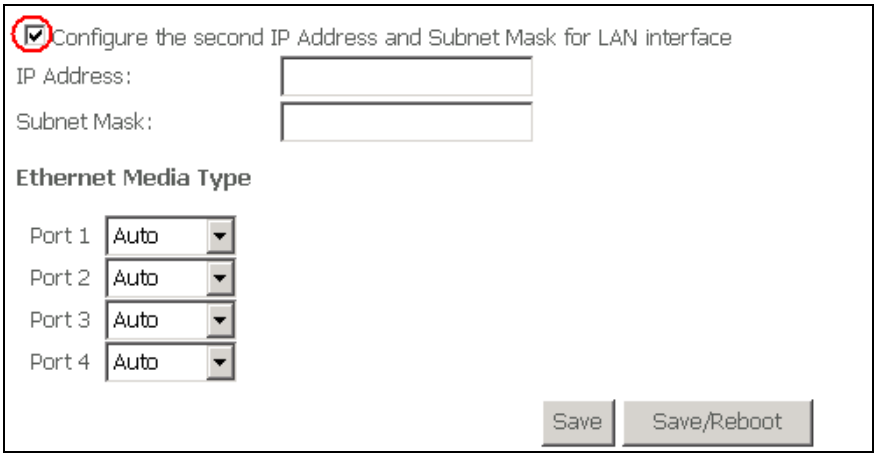
Standard Mode**:** In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group – even if IGMP snooping is enabled.

Blocking Mode**:** In blocking mode, the multicast data traffic will be blocked and not flood to all bridge ports when there are no client subscriptions to any multicast group.

DHCP Server: To enable DHCP, select **Enable DHCP server** and enter starting and ending IP addresses and the leased time. This setting configures the router to automatically assign IP, default gateway and DNS server addresses to every PC on your LAN.

DHCP Server Relay: Enable with checkbox ☑ and enter DHCP Server IP address. This allows the Router to relay the DHCP packets to the remote DHCP server. The remote DHCP server will provide the IP address. *This option is hidden if NAT is enabled*

To configure a secondary IP address, tick the checkbox ☑ outlined (in RED) below.



IP Address: Enter the secondary IP address for the LAN port.

Subnet Mask: Enter the secondary subnet mask for the LAN port.

Ethernet Media Type
Select between Auto, 10_Half, 10_Full, 100_Half and 100_Full options.

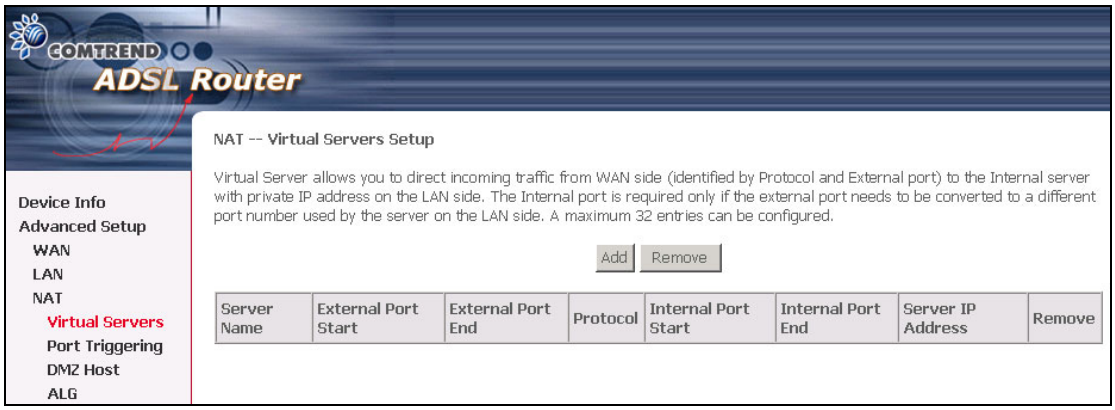
NOTE:	The **Save** button simply saves changes, while the **Save/Reboot** button both saves and reboots the device to make any changes effective.

6.3 NAT

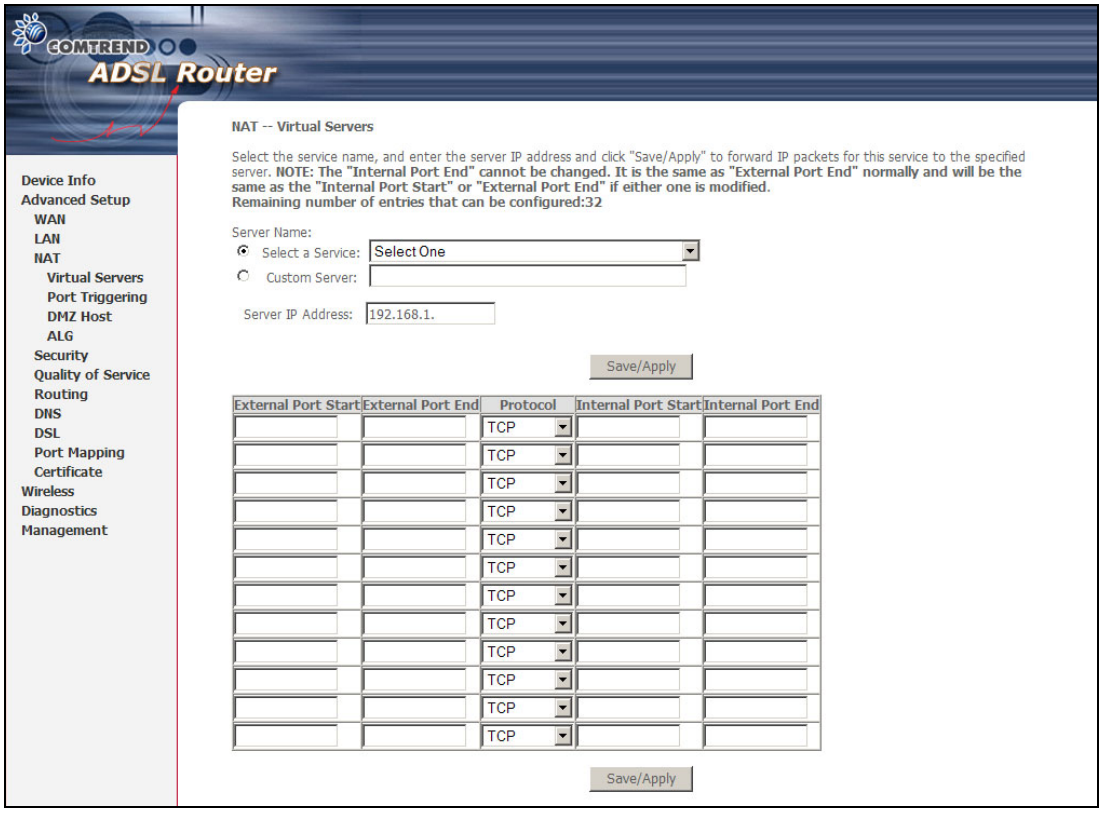
To display this option, NAT must be enabled in at least one PVC shown on the Advanced Setup - WAN screen. (*NAT is not an available option in Bridge mode*)

6.3.1 Virtual Servers

Virtual Servers allow you to direct incoming traffic from the WAN side (identified by Protocol and External port) to the Internal server with private IP addresses on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side.
A maximum of 32 entries can be configured.


COMTREND
ADSL Router
Device Info
Advanced Setup
WAN
LAN
NAT
Virtual Servers
Port Triggering
DMZ Host
ALG
NAT -- Virtual Servers Setup
Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.
Add
Remove
Server Name
External Port Start
External Port End
Protocol
Internal Port Start
Internal Port End
Server IP Address
Remove

To add a Virtual Server, click **Add**. The following will be displayed.

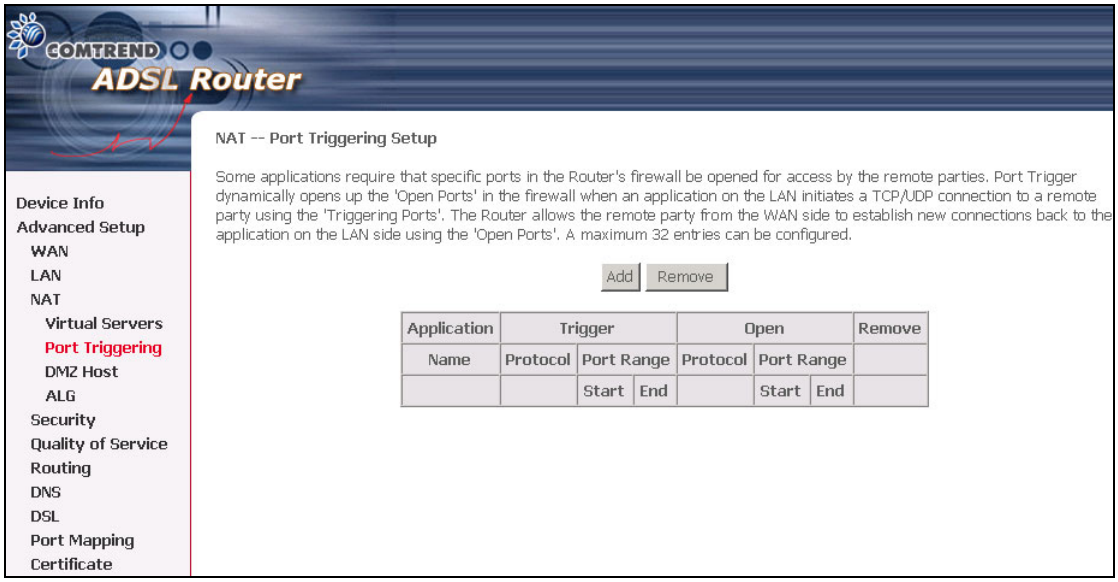


Consult the table below for field and header descriptions.

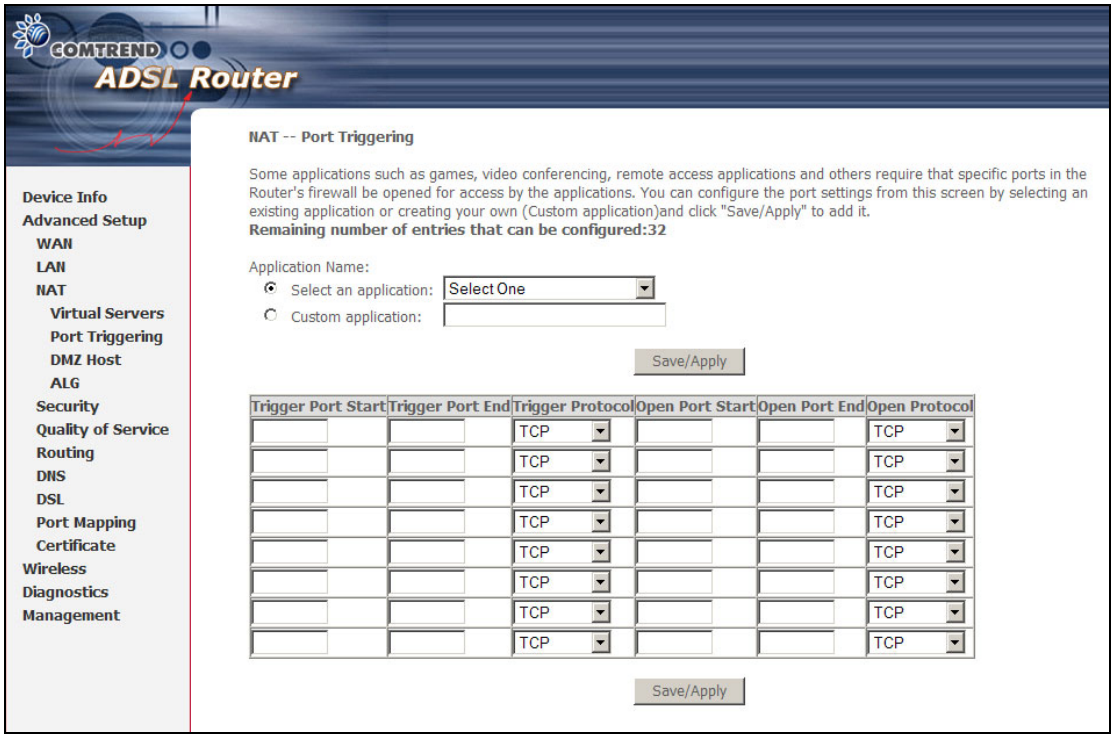
Field/Header	Description
Select a Service **Or** Custom Server	User should select the service from the list. Or User can enter the name of their choice.
Server IP Address	Enter the IP address for the server.
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.
Protocol	TCP, TCP/UDP, or UDP.
Internal Port Start	Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured
Internal Port End	Enter the internal port ending number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.

6.3.2 Port Triggering

Some applications require that specific ports in the firewall be opened for access by the remote parties. Port Triggers dynamically 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.



To add a Trigger Port, click **Add**. The following will be displayed.



Consult the table below for field and header descriptions.

Field/Header	Description
Select an Application **Or** Custom Application	User should select the application from the list. **Or** User can enter the name of their choice.
Trigger Port Start	Enter the starting trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Trigger Port End	Enter the ending trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Trigger Protocol	TCP, TCP/UDP, or UDP.
Open Port Start	Enter the starting open port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Open Port End	Enter the ending open port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Open Protocol	TCP, TCP/UDP, or UDP.

6.3.3 DMZ Host

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

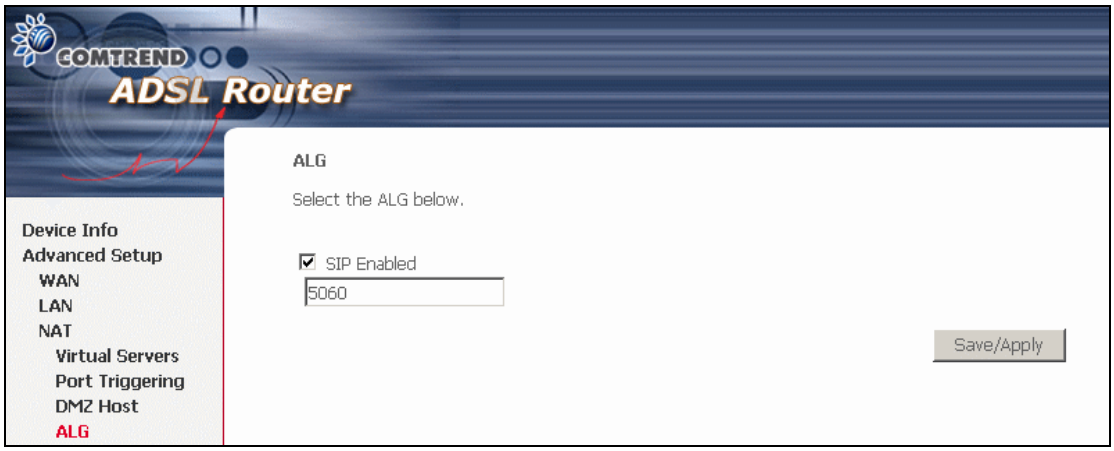
COMTREND
ADSL Router
Device Info
Advanced Setup
WAN
LAN
NAT
Virtual Servers
Port Triggering
DMZ Host
ALG
NAT -- DMZ Host
The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.
Enter the computer's IP address and click "Apply" to activate the DMZ host.
Clear the IP address field and click "Apply" to deactivate the DMZ host.
DMZ Host IP Address:
Save/Apply

To **Activate** the DMZ host, enter the DMZ host IP address and click **Save/Apply**.
To **Deactivate** the DMZ host, clear the IP address field and click **Save/Apply**.

6.3.4 ALG

Session Initiation Protocol (SIP - RFC3261) Application Layer Gateway (ALG) is the protocol of choice for most VoIP (Voice over IP) phones to initiate communication. If the user has an IP phone (SIP) or VoIP gateway (SIP) situated behind the router, the SIP ALG can help VoIP packets pass through when NAT is enabled.

Tick the **SIP Enabled** checkbox ☑ to enable SIP ALG. The text box defines the UDP port to be used (see NOTE below). Adjust settings and then click **Save/Apply**.



NOTE: This ALG is only valid for SIP protocol running on UDP port 5060.

6.4 Security

To display this function, you must enable the firewall feature in WAN Setup.
For detailed descriptions, with examples, please consult Appendix A: Firewall.

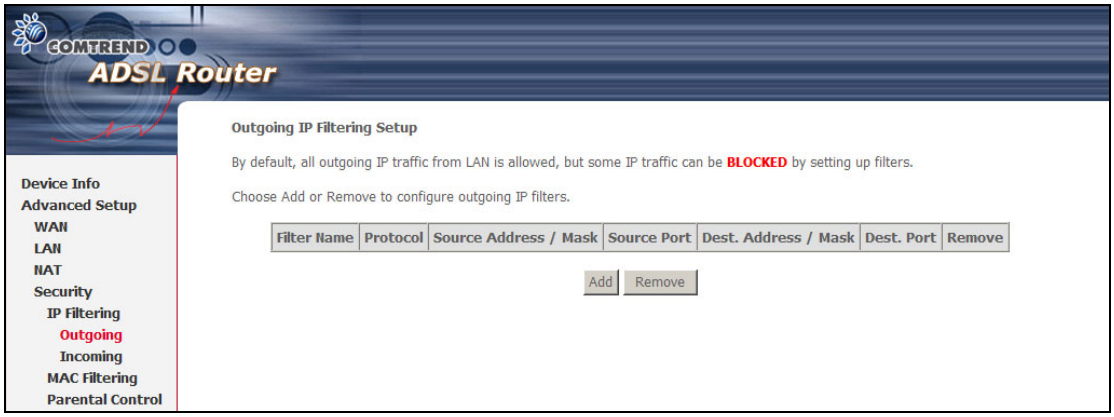
6.4.1 IP Filtering

This screen sets filter rules that limit IP traffic (Outgoing/Incoming). Multiple filter rules can be set and each applies at least one limiting condition. For individual IP packets to pass the filter all conditions must be fulfilled.

NOTE:	This function is not available when in bridge mode. Instead of IP Filtering, MAC Filtering (pg. 54) performs a similar function.

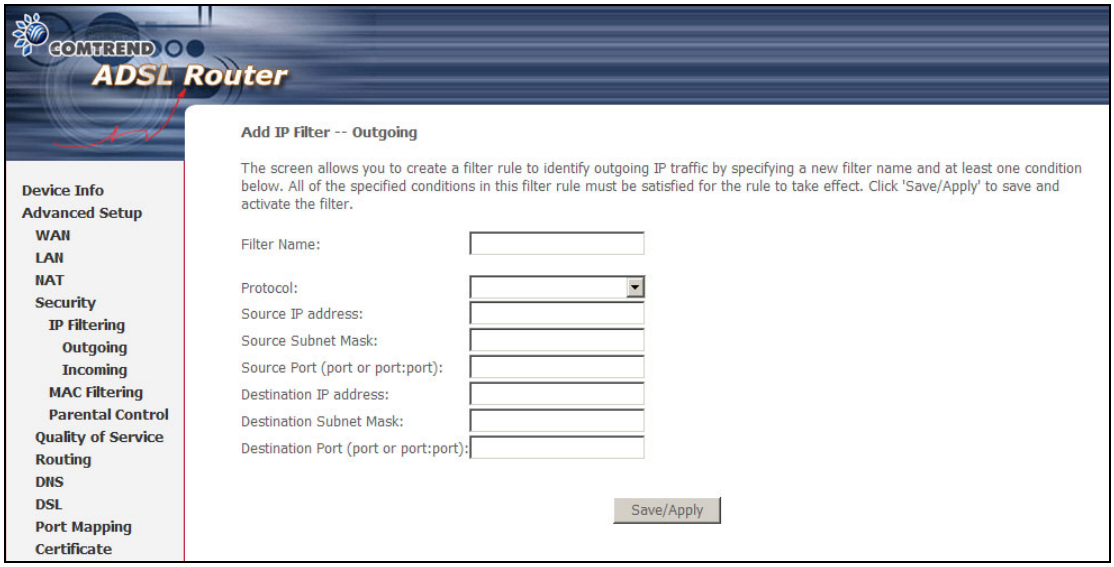
OUTGOING IP FILTER

By default, all outgoing IP traffic is allowed, but IP traffic can be blocked with filters.



To add a filter (to block some outgoing IP traffic), click the **Add** button.

On the following screen, enter your filter criteria and then click **Save/Apply**.

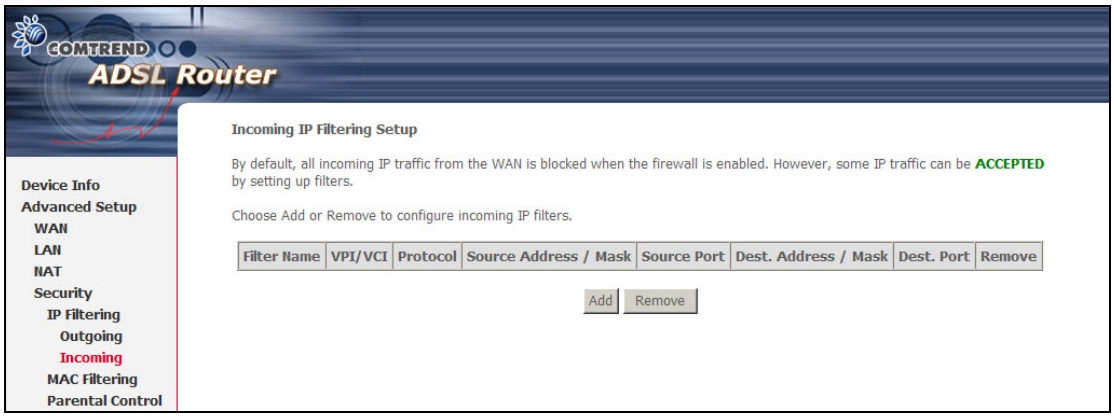


Consult the table below for field descriptions.

Field	Description
Filter Name	The filter rule label
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Source IP address	Enter source IP address.
Source Subnet Mask	Enter source subnet mask.
Source Port (port or port:port)	Enter source port number or range.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination port (port or port:port)	Enter destination port number or range.

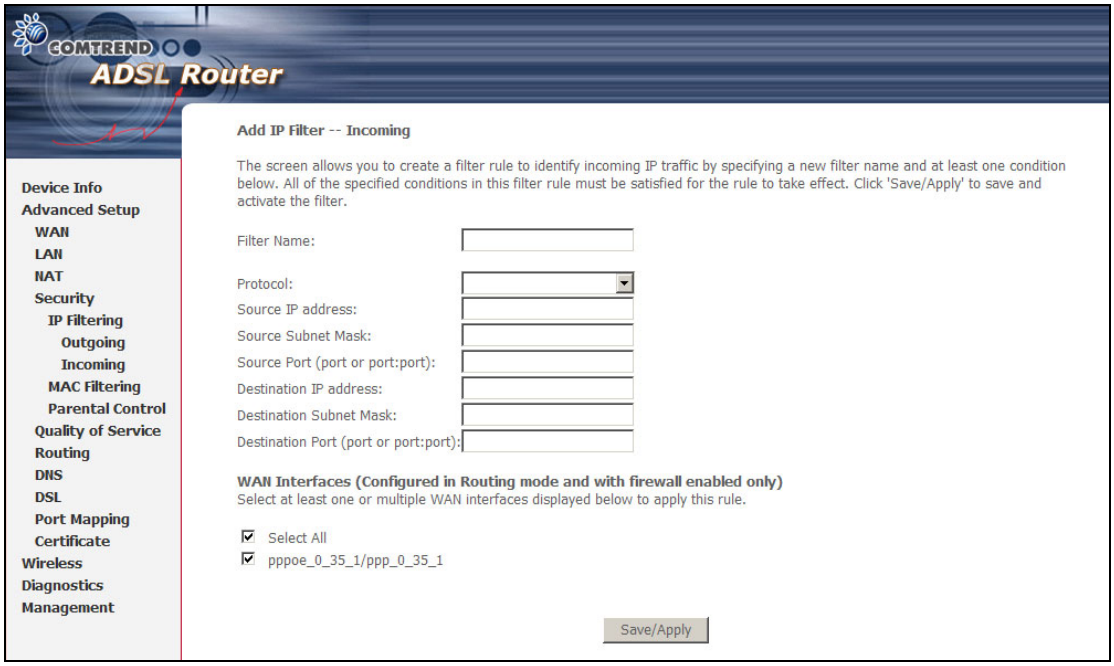
INCOMING IP FILTER

By default, all incoming IP traffic is blocked, but IP traffic can be allowed with filters.



To add a filter (to allow incoming IP traffic), click the **Add** button.

On the following screen, enter your filter criteria and then click **Save/Apply**.



For detailed field descriptions, please reference the previous table.

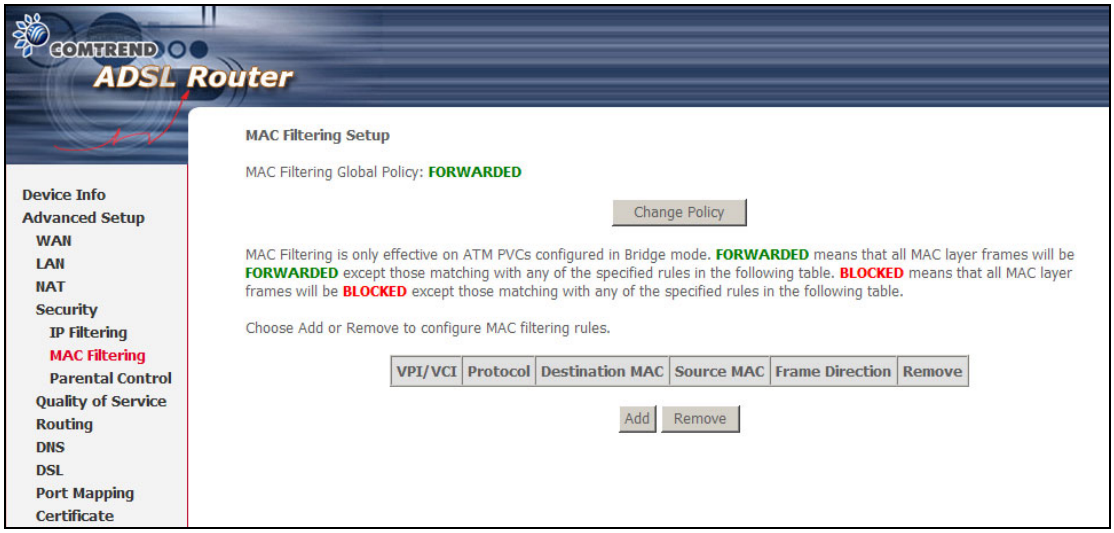
Under **WAN Interfaces**, select the PVCs (All routing modes with firewall ON) where the filter rule will apply. You may select all PVCs or just a subset. Filter rules are arranged by PVC as shown under the VPI/VCI heading on the previous screen.

6.4.2 MAC Filtering

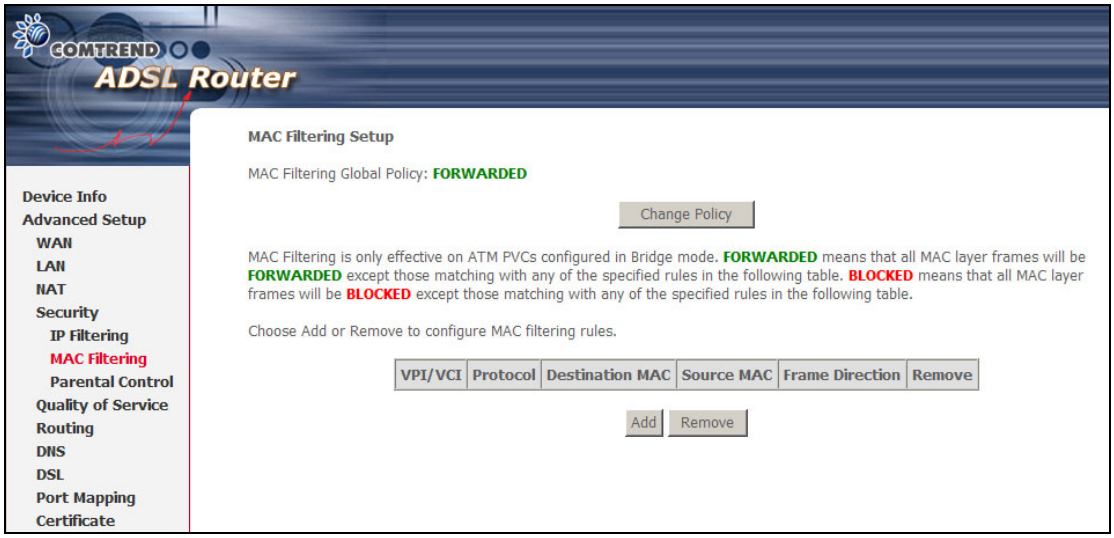
NOTE:	This option is only available in bridge mode. Other modes (i.e. PPPoE/A, IPoA, MER) use IP Filtering (pg. 52) to perform a similar function.

Each network device has a unique 48-bit MAC address. This can be used to filter (block or forward) packets based on the originating device. MAC filtering policy and rules for the CT-5361T can be set according to the following procedure.

The MAC Filtering Global Policy is defined as follows. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching the MAC filter rules. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching the MAC filter rules. The default MAC Filtering Global policy is **FORWARDED**. It can be changed by clicking the **Change Policy** button.



Choose **Add** or **Remove** to configure MAC filtering rules. The following screen will appear when you click **Add**. Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them must be met. Click **Save/Apply** to save and activate the filter rule.



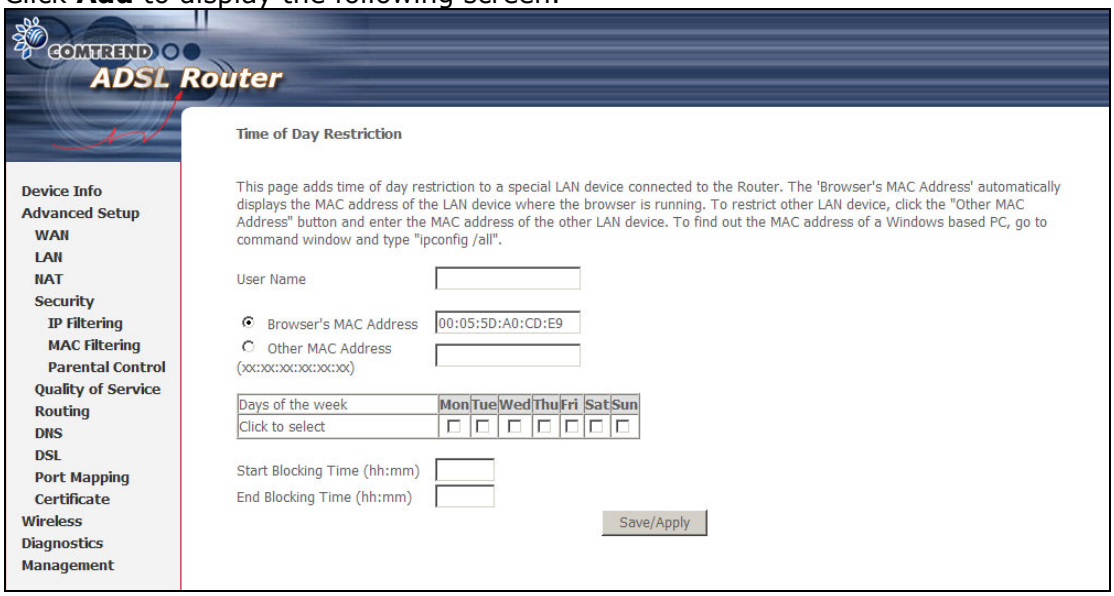
Consult the table below for detailed field descriptions.

Field	Description
Protocol Type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Defines the destination MAC address
Source MAC Address	Defines the source MAC address
Frame Direction	Select the incoming/outgoing packet interface
WAN Interfaces	Applies the filter to selected bridge PVCs. These rules are arranged according to bridge PVC, as shown under the VPI/VCI heading on the previous screen.

6.4.3 Parental Control

This feature restricts access from a LAN device to an outside network through the device on selected days at certain times. Make sure to activate the Internet Time server synchronization as described in section 9.5 Internet Time, so that the scheduled times match your local time.

Click **Add** to display the following screen.


COMTREND
ADSL Router
Time of Day Restriction
This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".
User Name
Browser's MAC Address
00:05:5D:A0:CD:E9
Other MAC Address
(xx:xx:xx:xx:xx:xx)
Days of the week
Mon Tue Wed Thu Fri Sat Sun
Click to select
Start Blocking Time (hh:mm)
End Blocking Time (hh:mm)
Save/Apply
Device Info
Advanced Setup
WAN
LAN
NAT
Security
IP Filtering
MAC Filtering
Parental Control
Quality of Service
Routing
DNS
DSL
Port Mapping
Certificate
Wireless
Diagnostics
Management

See below for field descriptions. Click **Save/Apply** to add a time restriction.

User Name: A user-defined label for this restriction.

Browser's MAC Address: MAC address of the PC running the browser.

Other MAC Address: MAC address of another LAN device.

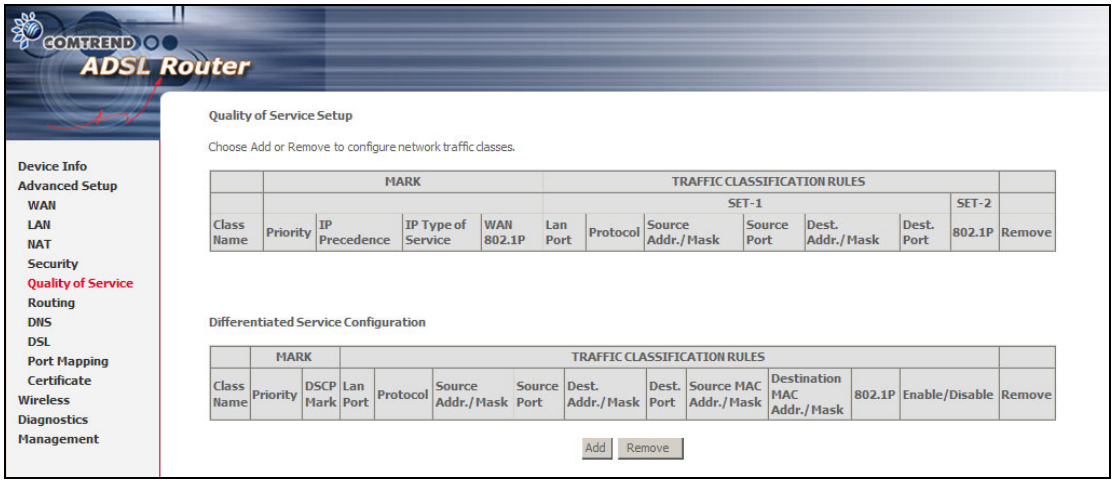
Days of the Week: The days the restrictions apply.

Start Blocking Time: The time the restrictions start.

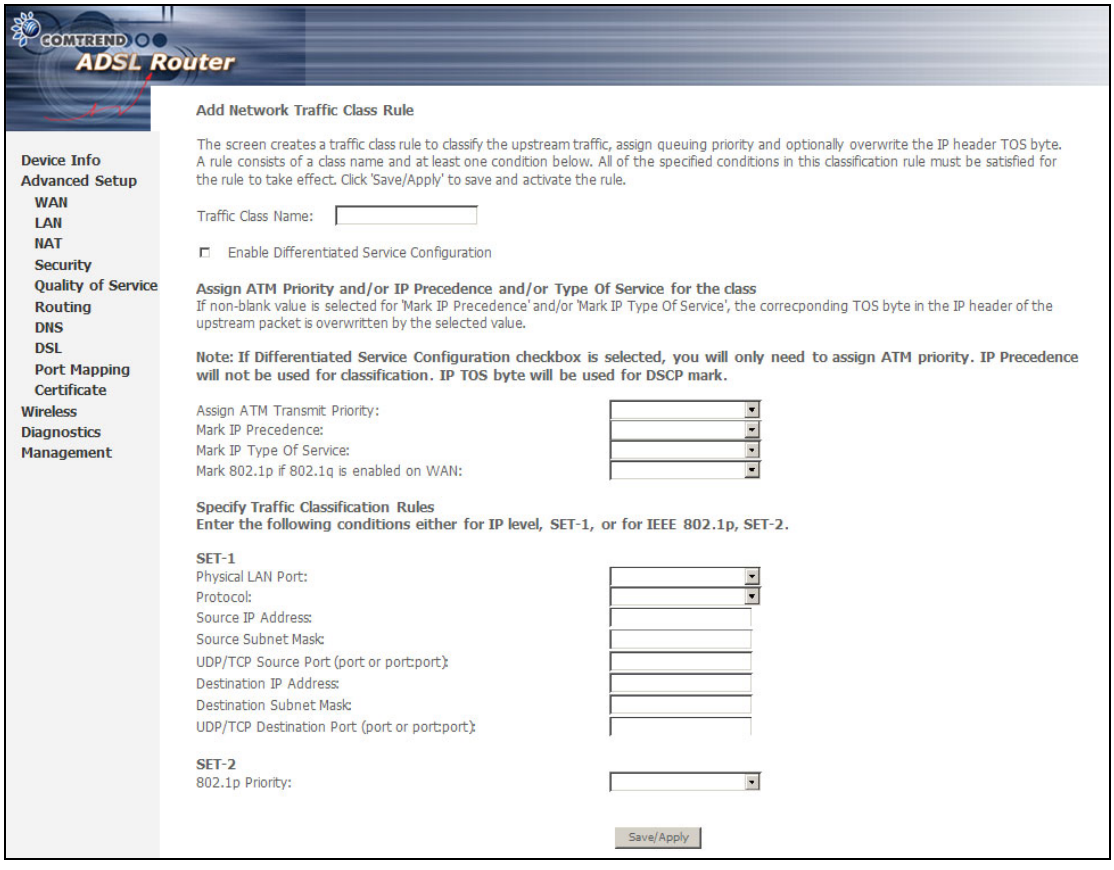
End Blocking Time: The time the restrictions end.

6.5 Quality of Service

NOTE: QoS must be enabled in at least one PVC to display this option. (see Advanced Setup - WAN for further instructions).



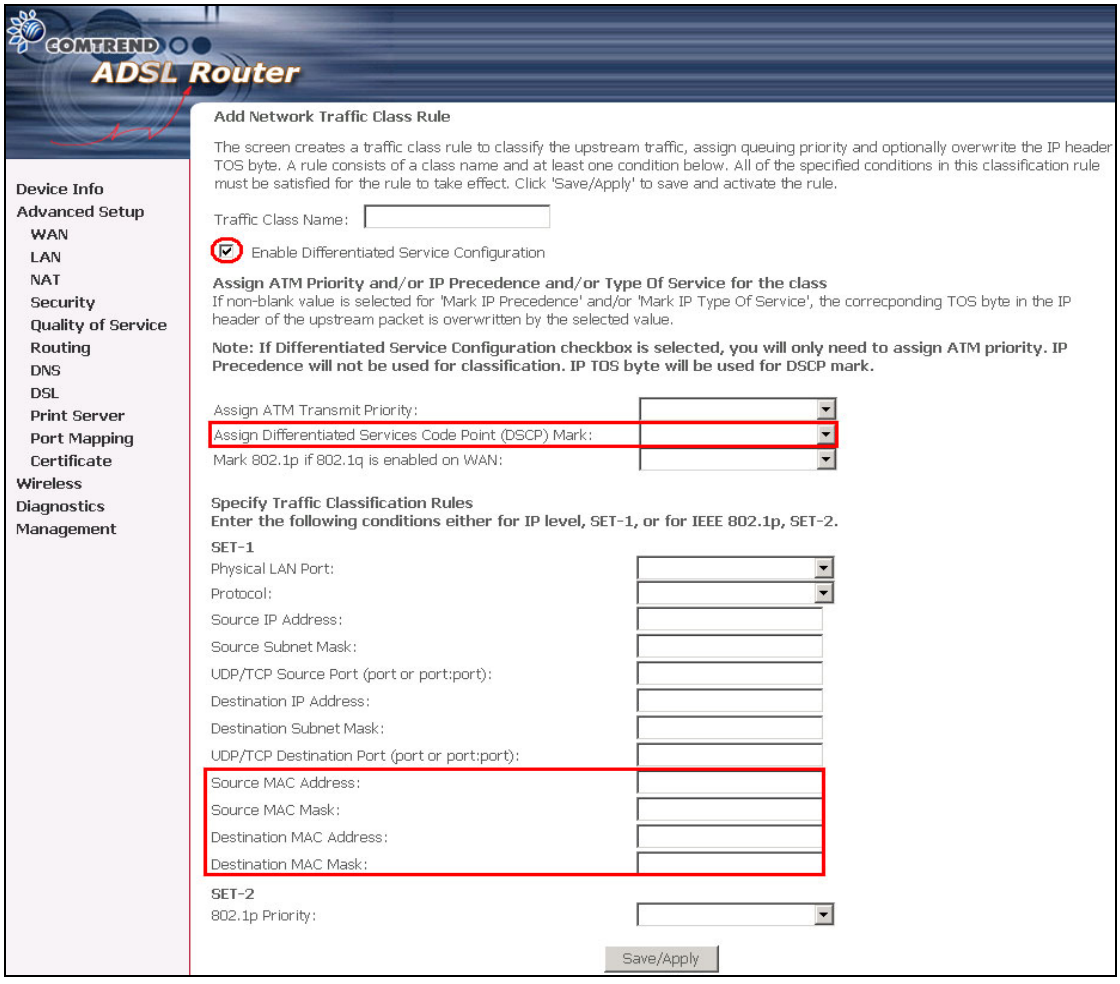
Choose **Add** to configure network traffic classes. The following screen will display.


COMTREND
ADSL Router
Add Network Traffic Class Rule
The screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DSL
Port Mapping
Certificate
Wireless
Diagnostics
Management
Traffic Class Name:
Enable Differentiated Service Configuration
Assign ATM Priority and/or IP Precedence and/or Type Of Service for the class
If non-blank value is selected for 'Mark IP Precedence' and/or 'Mark IP Type Of Service', the correcponding TOS byte in the IP header of the upstream packet is overwritten by the selected value.
Note: If Differentiated Service Configuration checkbox is selected, you will only need to assign ATM priority. IP Precedence will not be used for classification. IP TOS byte will be used for DSCP mark.
Assign ATM Transmit Priority:
Mark IP Precedence:
Mark IP Type Of Service:
Mark 802.1p if 802.1q is enabled on WAN:
Specify Traffic Classification Rules
Enter the following conditions either for IP level, SET-1, or for IEEE 802.1p, SET-2.
SET-1
Physical LAN Port:
Protocol:
Source IP Address:
Source Subnet Mask:
UDP/TCP Source Port (port or port:port):
Destination IP Address:
Destination Subnet Mask:
UDP/TCP Destination Port (port or port:port):
SET-2
802.1p Priority:
Save/Apply

Field	Description
Traffic Class Name	Enter name for traffic class.
Assign ATM Transmit Priority	Select Low, Medium or High.
Mark IP Precedence	Select between 0-7. The lower the digit shows the higher the priority.

Mark IP Type Of Service	Normal Service, Minimize Cost, Maximize Reliability, Maximize Throughput, Minimize Delay
Mark 802.1p if 802.1q is enabled on WAN	Select between 0-7. The higher the digit shows the higher the priority.
SET-1	
Physical LAN Port	Select between ENET(1-4) and USB
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the subnet mask for the source IP address.
UDP/TCP Source Port (port or port:port)	Enter source port number or port range.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
UDP/TCP Destination port (port or port:port)	Enter destination port number or port range.
SET-2	
802.1p Priority	Select between 0-7. The lower the digit shows the higher the priority

If the **Enable Differentiated Service Configuration** checkbox ☑ is selected, some additional fields will display, as shown below.


COMTREND
ADSL Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DSL
Print Server
Port Mapping
Certificate
Wireless
Diagnostics
Management
Add Network Traffic Class Rule
The screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.
Traffic Class Name:
Enable Differentiated Service Configuration
Assign ATM Priority and/or IP Precedence and/or Type Of Service for the class
If non-blank value is selected for 'Mark IP Precedence' and/or 'Mark IP Type Of Service', the correcponding TOS byte in the IP header of the upstream packet is overwritten by the selected value.
Note: If Differentiated Service Configuration checkbox is selected, you will only need to assign ATM priority. IP Precedence will not be used for classification. IP TOS byte will be used for DSCP mark.
Assign ATM Transmit Priority:
Assign Differentiated Services Code Point (DSCP) Mark:
Mark 802.1p if 802.1q is enabled on WAN:
Specify Traffic Classification Rules
Enter the following conditions either for IP level, SET-1, or for IEEE 802.1p, SET-2.
SET-1
Physical LAN Port:
Protocol:
Source IP Address:
Source Subnet Mask:
UDP/TCP Source Port (port or port:port):
Destination IP Address:
Destination Subnet Mask:
UDP/TCP Destination Port (port or port:port):
Source MAC Address:
Source MAC Mask:
Destination MAC Address:
Destination MAC Mask:
SET-2
802.1p Priority:
Save/Apply

The additional Items are explained here.

Assign Differentiated Services Code Point (DSCP) Mark	The selected Code Point gives the corresponding priority to the packets that satisfies the rules set below.
Source MAC Address	A packet belongs to SET-1, if a binary-AND of its source MAC address with the Source MAC Mask is equal to the binary-AND of the Source MAC Mask and this field.
Source MAC Mask	This is the mask used to decide how many bits are checked in Source MAC Address.
Destination MAC Address	A packet belongs to SET-1 then the result that the Destination MAC Address of its header binary-AND to the Destination MAC Mask must equal to the result that this field binary-AND to the Destination MAC Mask.
Destination MAC Mask	This is the mask used to decide how many bits are checked in Destination MAC Address.

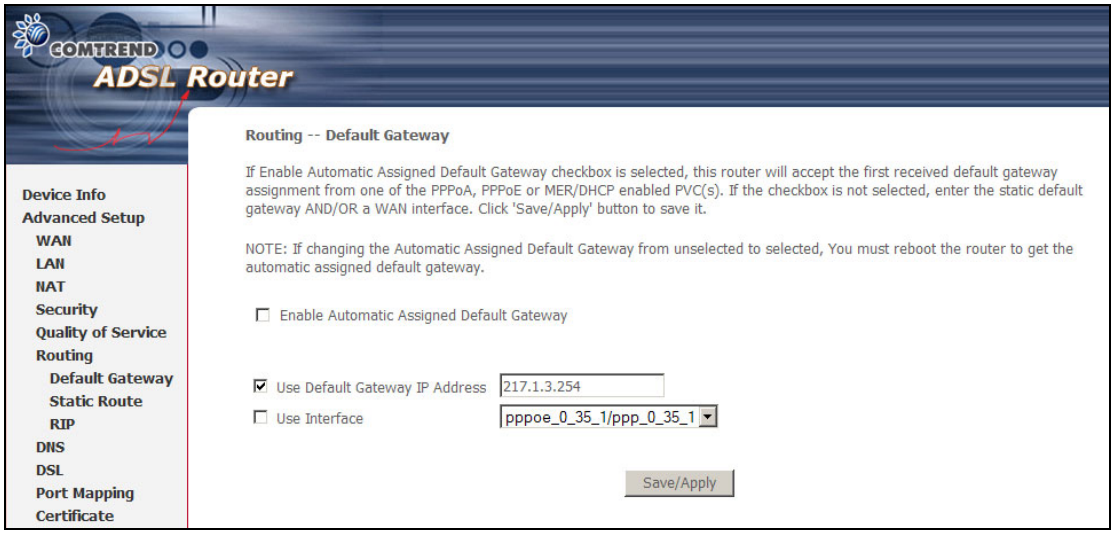
6.6 Routing

This option allows for **Default Gateway, Static Route,** and **RIP** configuration.

NOTE:	In bridge mode, the **RIP** screen is hidden while the **Default Gateway** and **Static Route** configuration screens are shown but ineffective.

6.6.1 Default Gateway

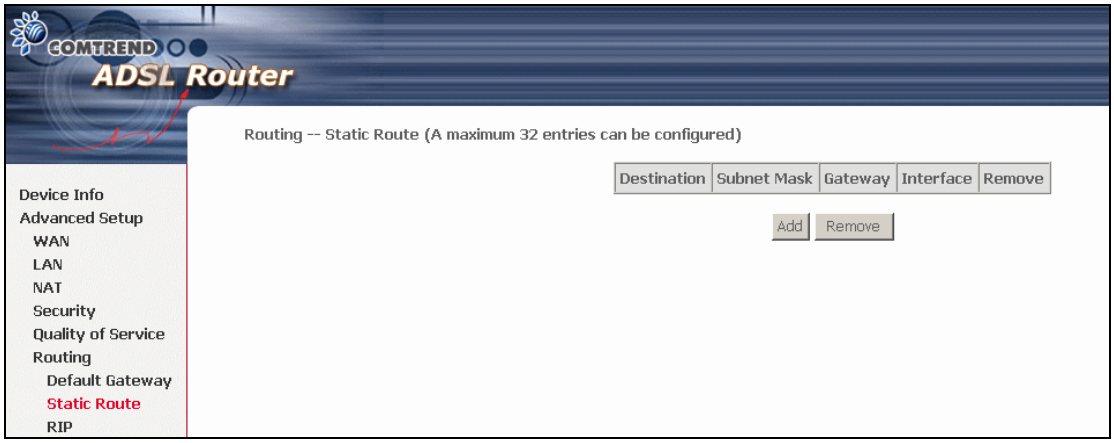
If the **Enable Automatic Assigned Default Gateway** checkbox ☑ is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox ☑ is not selected, enter the static default gateway AND/OR a WAN interface. Click **Save/Apply.**


COMTREND
ADSL Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
Default Gateway
Static Route
RIP
DNS
DSL
Port Mapping
Certificate
Routing -- Default Gateway
If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.
NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.
Enable Automatic Assigned Default Gateway
Use Default Gateway IP Address
217.1.3.254
Use Interface
pppoe_0_35_1/ppp_0_35_1
Save/Apply

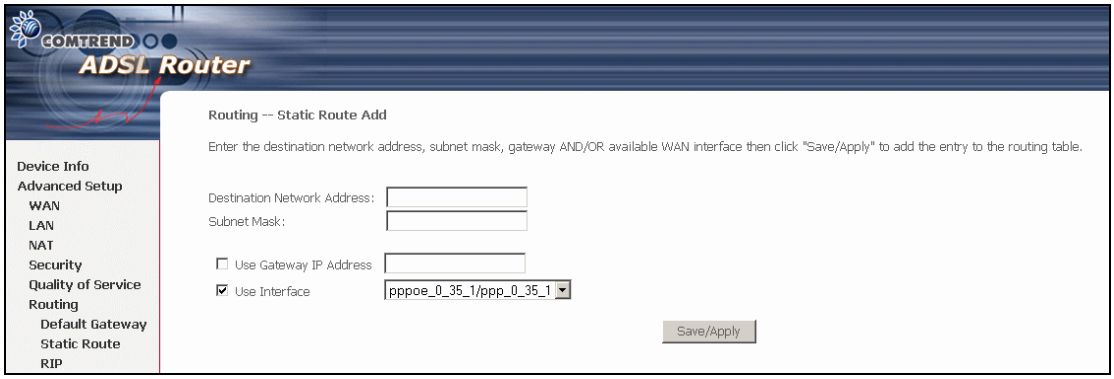
NOTE: After enabling the Automatic Assigned Default Gateway, the device must be rebooted to activate the assigned default gateway.

6.6.2 Static Route

This option allows for the configuration of static routes. Click **Add** to create a new static route. Click **Remove** to delete the selected static route.



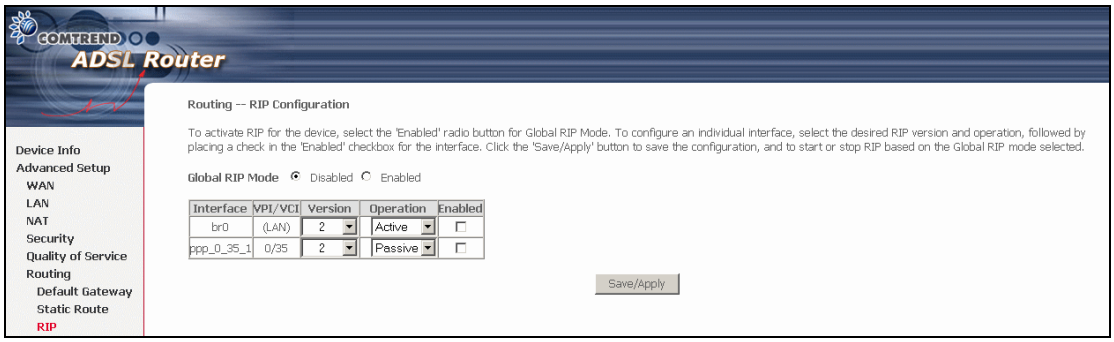
Click the **Add** button to display the following screen.



Enter Destination Network Address, Subnet Mask, Gateway IP Address, and/or WAN Interface. Then click **Save/Apply** to add the entry to the routing table.

6.6.3 RIP

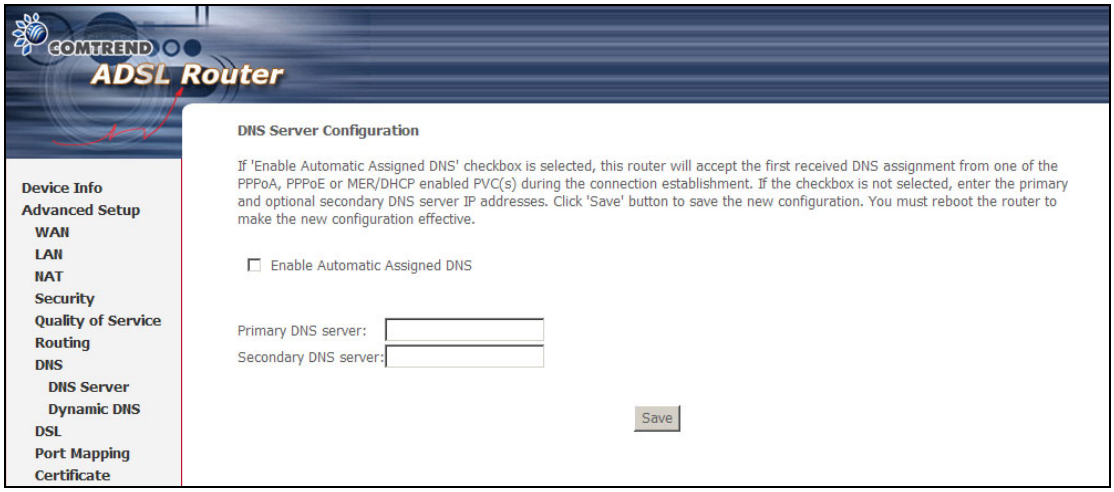
To activate RIP, select the **Enabled** radio button for Global RIP Mode. To configure an individual interface (PVC), select the desired RIP version and operation, and then select the **Enabled** checkbox ☑ for that interface (PVC). Click **Save/Apply** to save the configuration and start/stop RIP (based on the Global RIP mode selected).



6.7 DNS

6.7.1 DNS Server

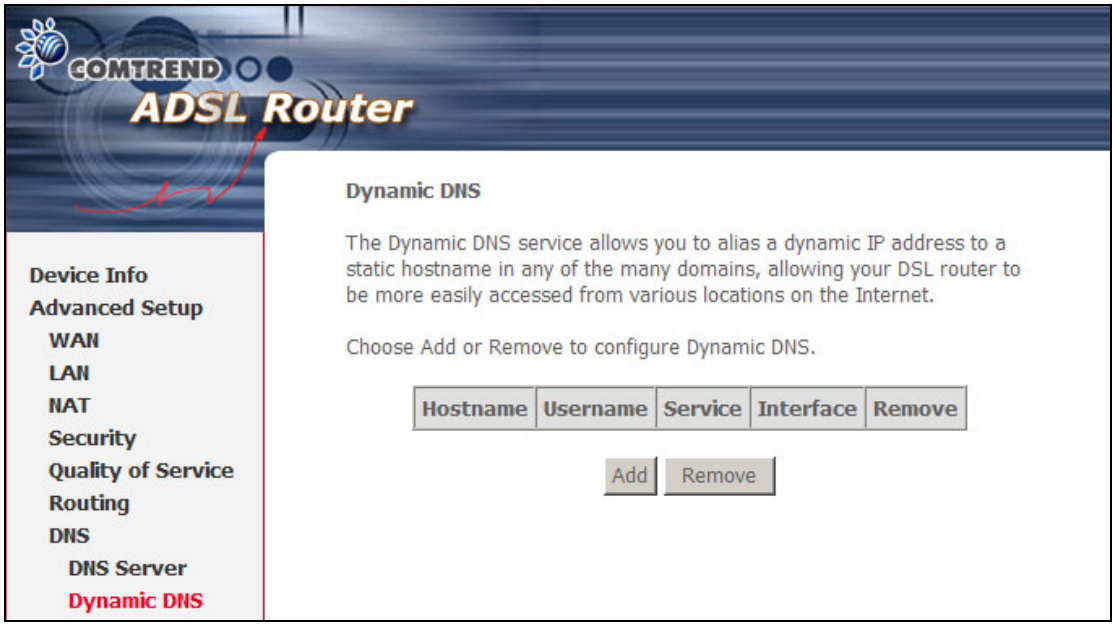
If the **Enable Automatic Assigned DNS** checkbox ☑ is selected, this router will accept the first received DNS assignment from one of the DHCP enabled PVC(s). If the checkbox ☑ is not selected, enter the primary and optional secondary DNS server IP addresses. Click **Save** to save the new configuration.


COMTREND
ADSL Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DNS Server
Dynamic DNS
DSL
Port Mapping
Certificate
DNS Server Configuration
If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the router to make the new configuration effective.
Enable Automatic Assigned DNS
Primary DNS server:
Secondary DNS server:
Save

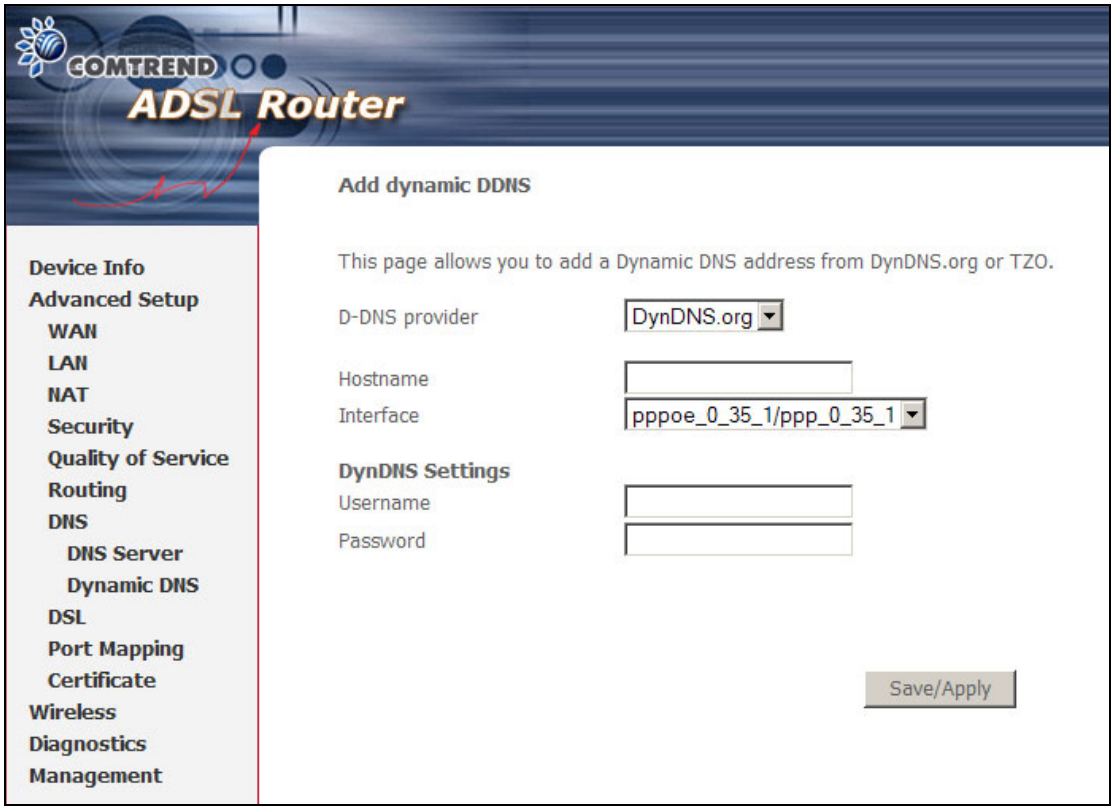
NOTE:	You must reboot the router to make the new configuration effective.

6.7.2 Dynamic DNS

The Dynamic DNS service allows you to map a dynamic IP address to a static hostname in any of many domains, allowing the CT-5361T to be more easily accessed from various locations on the Internet.



To add a dynamic DNS service, click **Add**. The following screen will display.

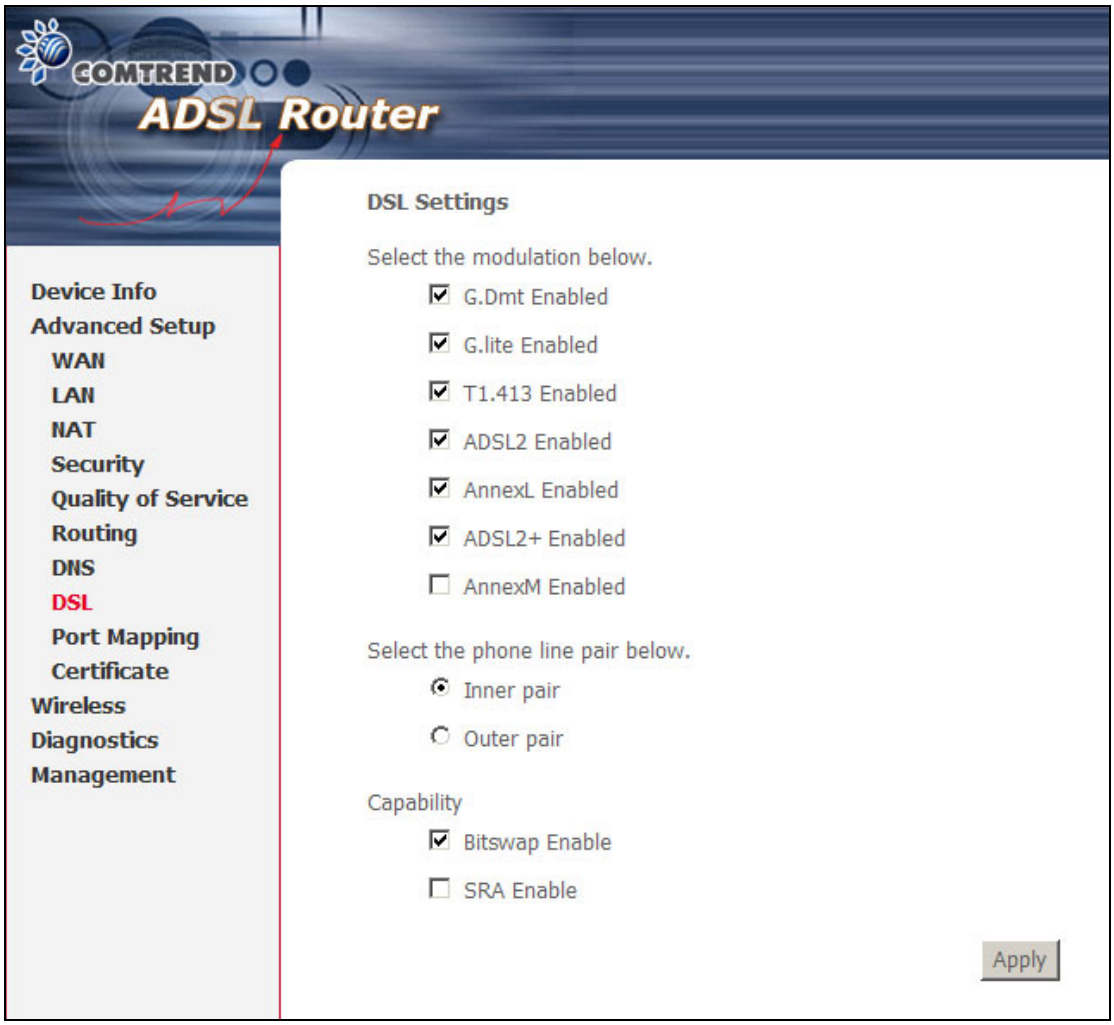


Consult the table below for field descriptions.

Field	Description
D-DNS provider	Select a dynamic DNS provider from the list
Hostname	Enter the name for the dynamic DNS server
Interface	Select the interface (PVC) from the list
Username	Enter the username for the dynamic DNS server
Password	Enter the password for the dynamic DNS server

6.8 DSL

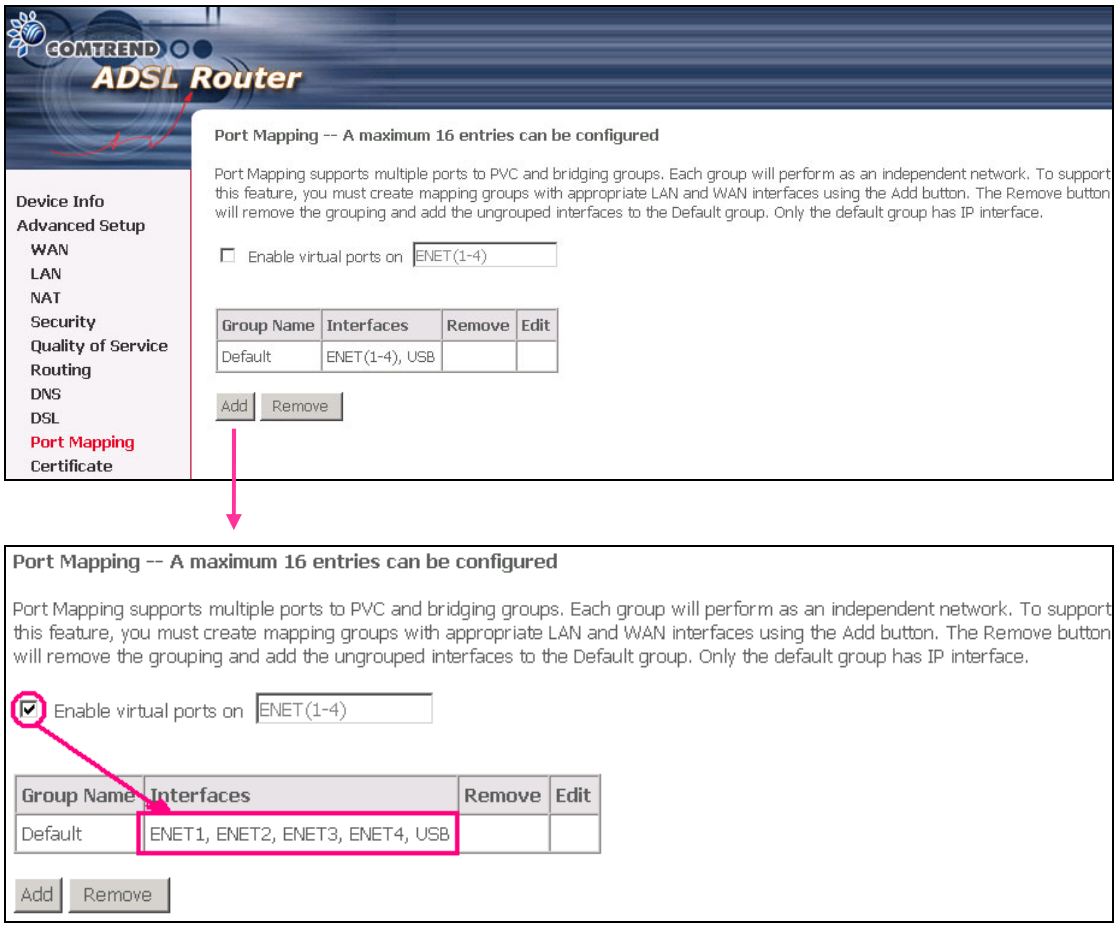
The DSL Settings screen allows for the selection of DSL modulation modes.
For optimum performance, the modes selected should match those of your ISP.



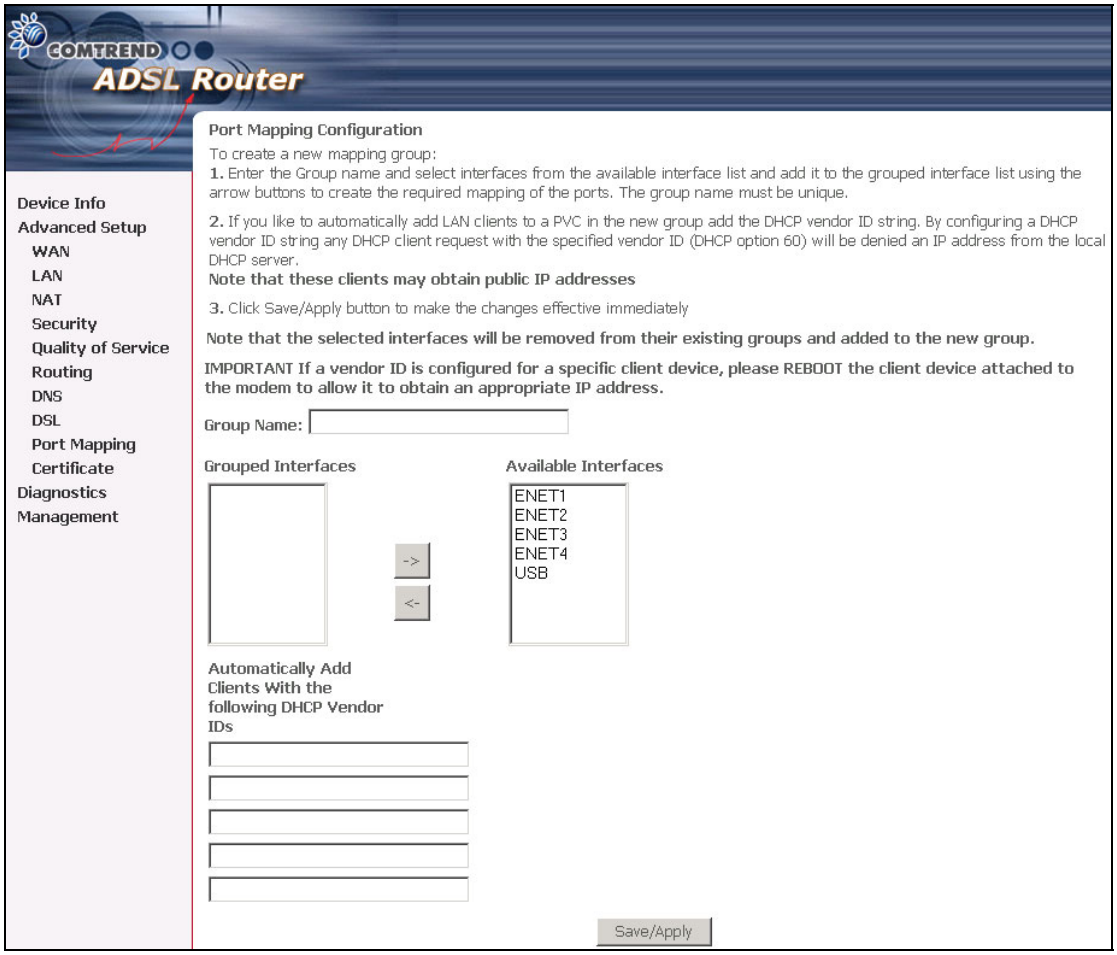
DSL Mode	**Data Transmission Rate** - Mbit/s (Megabits per second)
G.Dmt	Downstream: 12 Mbit/s Upstream: 1.3 Mbit/s
G.lite	Downstream: 4 Mbit/s Upstream: 0.5 Mbit/s
T1.413	Downstream: 8 Mbit/s Upstream: 1.0 Mbit/s
ADSL2	Downstream: 12 Mbit/s Upstream: 1.0 Mbit/s
AnnexL	Supports longer loops but with reduced transmission rates
ADSL2+	Downstream: 24 Mbit/s Upstream: 1.0 Mbit/s
AnnexM	Downstream: 24 Mbit/s Upstream: 3.5 Mbit/s
Options	**Description**
Inner/Outer Pair	Select the inner or outer pins of the twisted pair (RJ11 cable)
Bitswap Enable	Enables adaptive handshaking functionality
SRA Enable	Enables Seamless Rate Adaptation (SRA)

6.9 Port Mapping

Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To use this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the **Add** button. The **Remove** button acts to remove mapping groups and return the ungrouped interfaces to the Default group. As shown below, when you tick the **Enable virtual ports on**, the LAN interfaces (ENET1-4) in the default group will separate.


COMTREND
ADSL Router
Port Mapping -- A maximum 16 entries can be configured
Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DSL
Port Mapping
Certificate
Enable virtual ports on
ENET(1-4)
Group Name
Interfaces
Remove
Edit
Default
ENET(1-4), USB
Add
Remove
Port Mapping -- A maximum 16 entries can be configured
Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.
Enable virtual ports on
ENET(1-4)
Group Name
Interfaces
Remove
Edit
Default
ENET1, ENET2, ENET3, ENET4, USB
Add
Remove

To add a port-mapping group, click **Add**.


COMTREND
ADSL Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DSL
Port Mapping
Certificate
Diagnostics
Management
Port Mapping Configuration
To create a new mapping group:
1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.
2. If you like to automatically add LAN clients to a PVC in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
Note that these clients may obtain public IP addresses
3. Click Save/Apply button to make the changes effective immediately
Note that the selected interfaces will be removed from their existing groups and added to the new group.
IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.
Group Name:
Grouped Interfaces
Available Interfaces
ENET1
ENET2
ENET3
ENET4
USB
->
<-
Automatically Add Clients With the following DHCP Vendor IDs
Save/Apply

To create a group from the list, first enter the group name and then select from the available interfaces on the list.

Automatically Add Clients With the Following DHCP Vendor IDs:
Add support to automatically map LAN interfaces to PVC's using DHCP vendor ID (option 60). The local DHCP server will decline and send the requests to a remote DHCP server by mapping the appropriate LAN interface. This will be turned on when Port Mapping is enabled.

There are 4 PVCs (0/33, 0/36, 0/37, 0/38). 0/33 is for PPPoE and the others are for IP setup-box (video). The LAN interfaces are ETH1, ETH2, ETH3, ETH4, and USB. Port mapping configuration is:

1. Default: ENET1, ENET2, ENET3, ENET4, and USB.
2. Video: nas_0_36, nas_0_37, and nas_0_38. The DHCP vendor ID is "Video".

The CPE's DHCP server is running on "Default" and ISP's DHCP server is running on PVC 0/36. It is for setup-box use only. On the LAN side, PC can get IP address from CPE's DHCP server and access Internet via PPPoE (0/33).

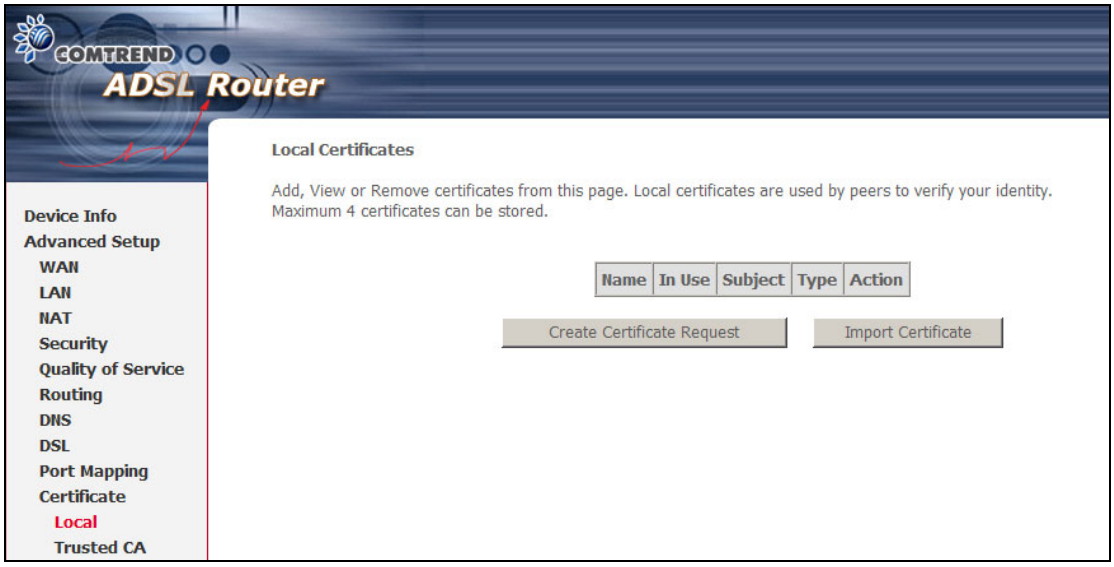
If the setup-box is connected with interface "ENET1" and sends a DHCP request with vendor id "Video", the CPE's DHCP server will forward this request to ISP's DHCP server. CPE will change the port-mapping configuration automatically. The port-mapping configuration will become:

1. Default: ENET2, ENET3, ENET4, and USB.
2. Video: nas_0_36, nas_0_37, nas_0_38, and ENET1.

6.10 Certificate

A certificate is a public key, attached with its owner's information (company name, server name, personal real name, contact e-mail, postal address, etc) and digital signatures. There will be one or more digital signatures attached to the certificate, indicating that these entities have verified that this certificate is valid.

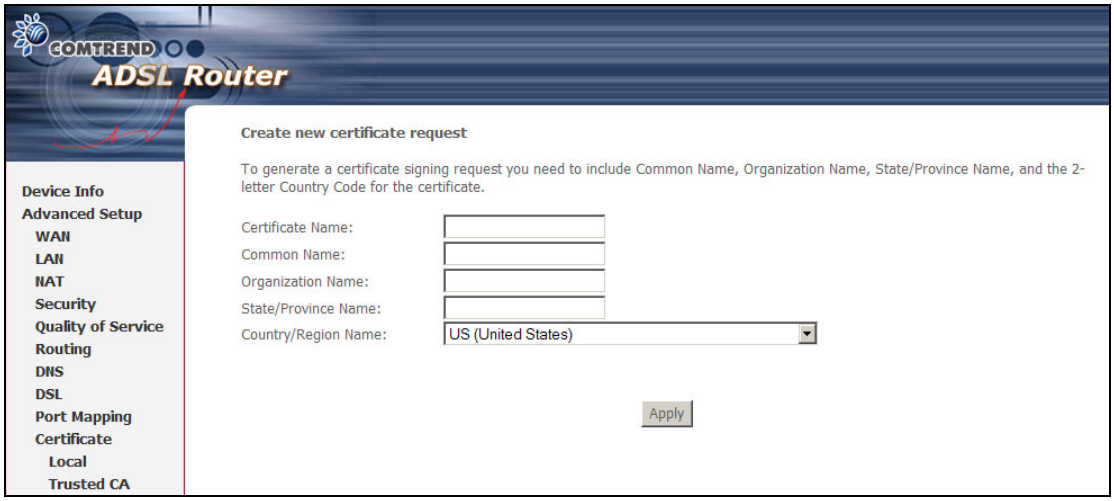
6.10.1 Local



CREATE CERTIFICATE REQUEST

Click **Create Certificate Request** to generate a certificate-signing request.

The certificate-signing request can be submitted to the vendor/ISP/ITSP to apply for a certificate. Some information must be included in the certificate-signing request. Your vendor/ISP/ITSP will ask you to provide the information they require and to provide the information in the format they regulate. Enter the required information and click **Apply** to generate a private key and a certificate-signing request.

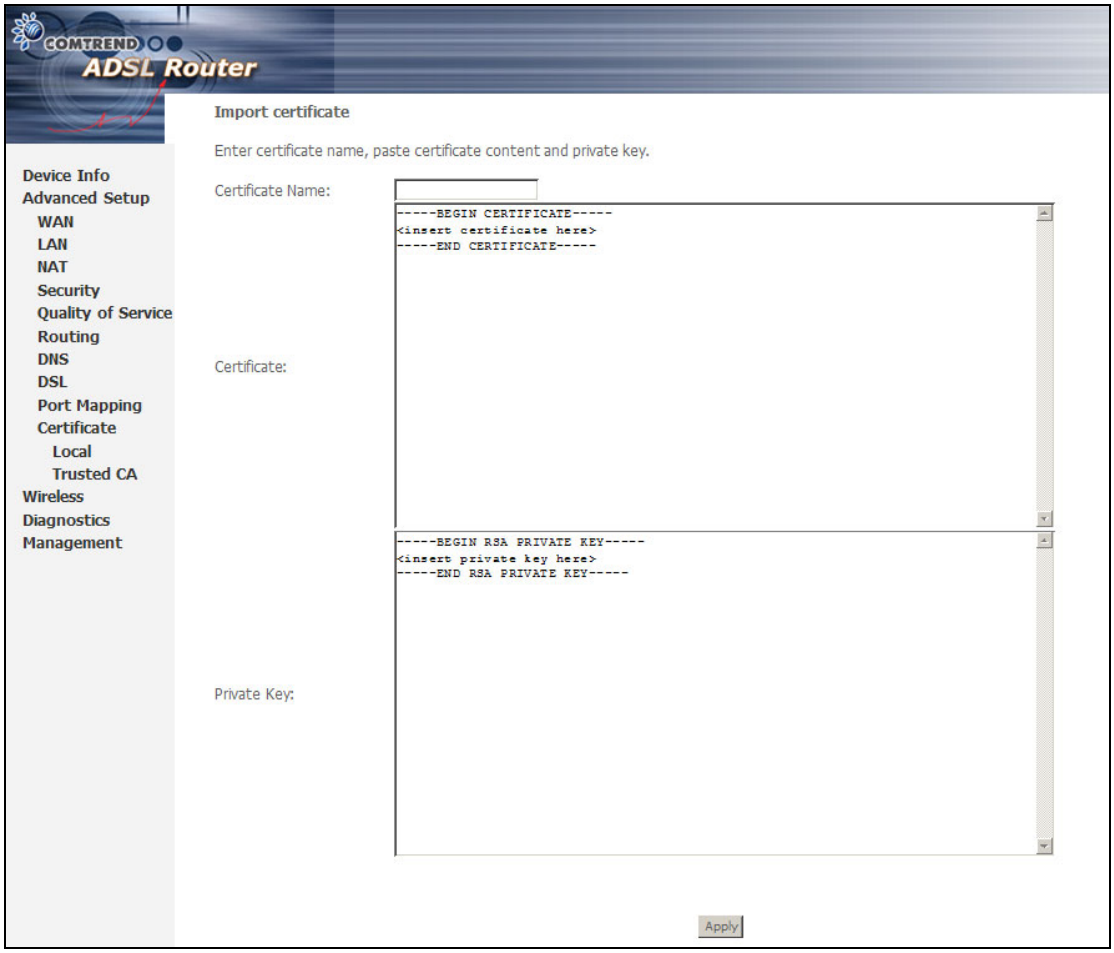


The following table is provided for your reference.

Field	Description
Certificate Name	A user-defined name for the certificate.
Common Name	Usually, the fully qualified domain name for the machine.
Organization Name	The exact legal name of your organization. Do not abbreviate.
State/Province Name	The state or province where your organization is located. It cannot be abbreviated.
Country/Region Name	The two-letter ISO abbreviation for your country.

IMPORT CERTIFICATE

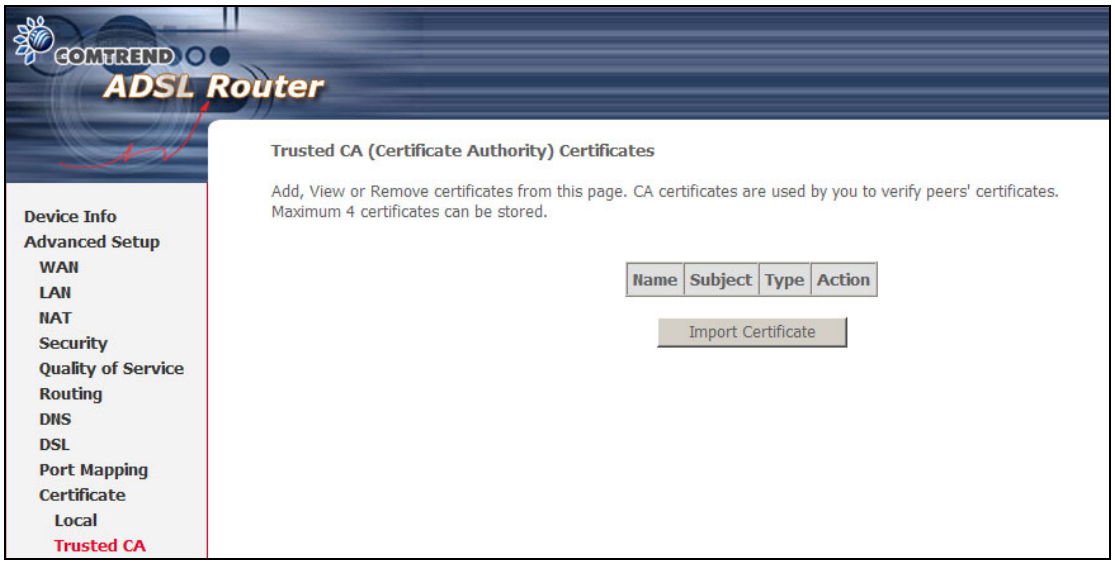
Click **Import Certificate** to paste the certificate content and the private key provided by your vendor/ISP/ITSP into the corresponding boxes shown below.



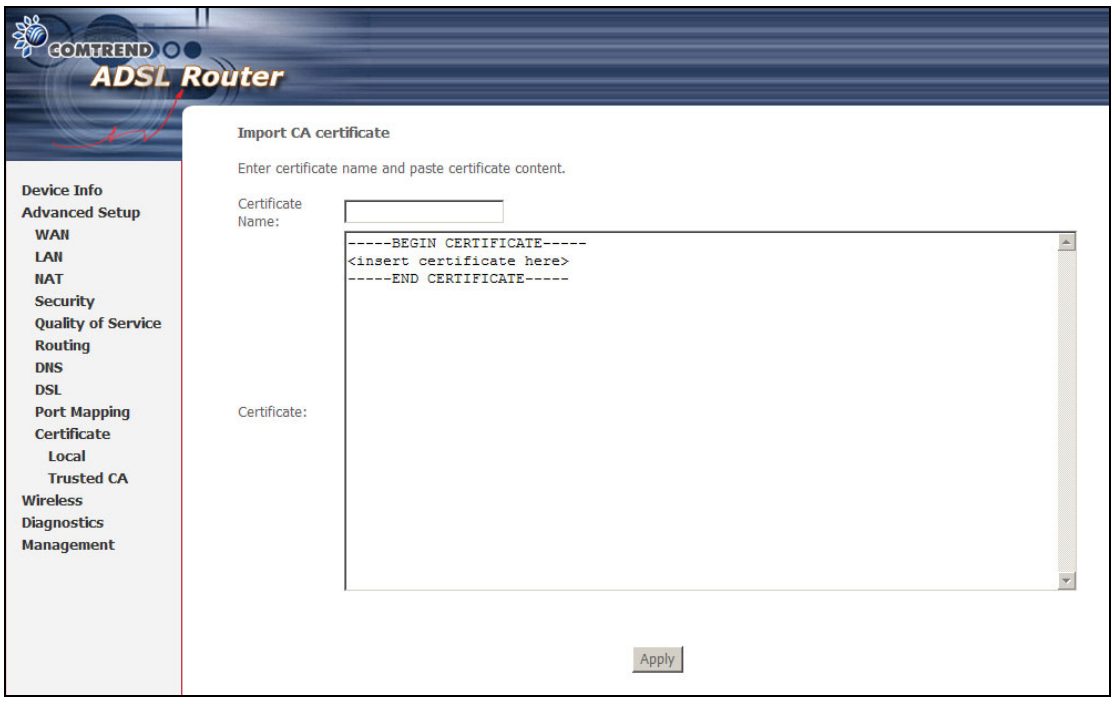
Enter a certificate name and click **Apply** to import the certificate.

6.10.2 Trusted CA

CA is an abbreviation for Certificate Authority, which is a part of the X.509 system. It is itself a certificate, attached with the owner information of this certificate authority; but its purpose is not encryption/decryption. Its purpose is to sign and issue certificates, in order to prove that these certificates are valid.



Click **Import Certificate** to paste the certificate content of your trusted CA. The CA certificate content will be provided by your vendor/ISP/ITSP and is used to authenticate the Auto-Configuration Server (ACS) that the CPE will connect to.



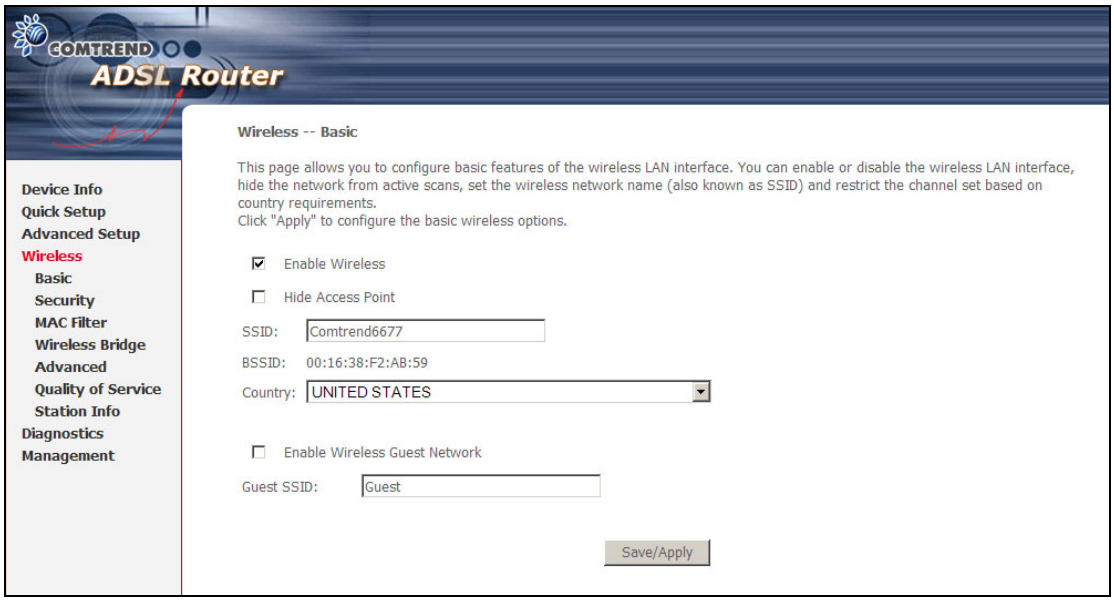
Enter a certificate name and click **Apply** to import the CA certificate.

Chapter 7 Wireless

The Wireless menu provides access to the wireless options discussed below.

7.1 Basic

The Basic option allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.



Click **Save/Apply** to apply the selected wireless options.

Consult the table below for descriptions of these options.

Option	Description
Enable Wireless	A checkbox ☑ that enables or disables the wireless LAN interface. When selected, a set of basic wireless options will appear.
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. To check AP status in Windows XP, open **Network Connections** from the **start** Menu and select **View Available Network Connections**. If the access point is hidden, it will not be listed there. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration.
SSID [1-32 characters]	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
BSSID	The BSSID is a 48-bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Media Access Control) address of the AP (Access Point); and in Independent BSS or ad hoc networks, the BSSID is generated randomly.

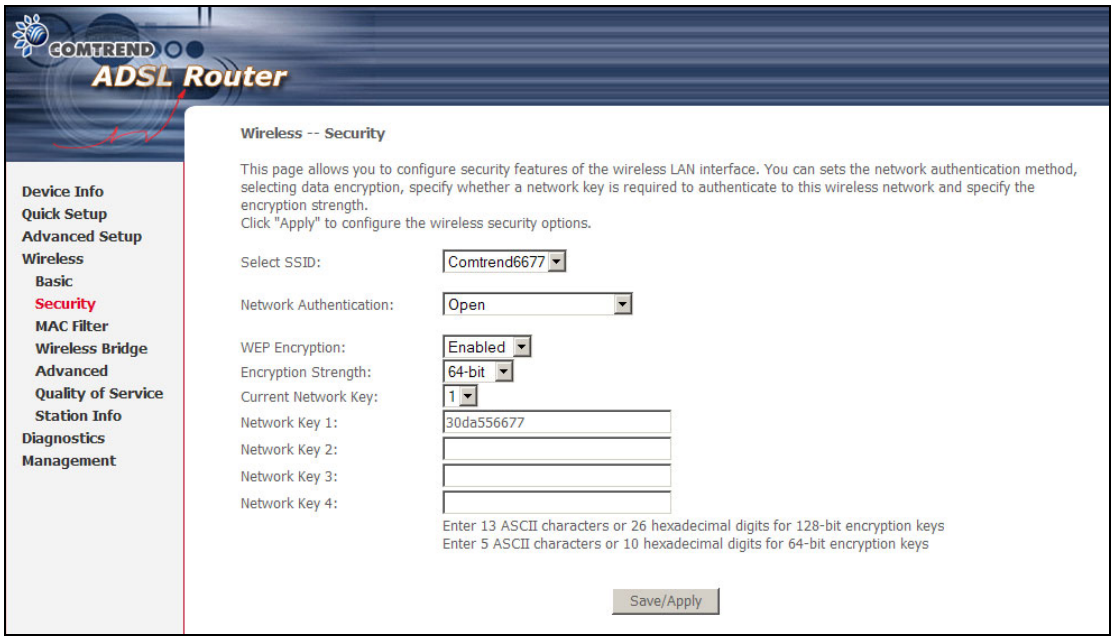
Country	A drop-down menu that permits worldwide and specific national settings. Each county listed below enforces specific regulations limiting channel range: US= worldwide, Japan=1-14, Jordan= 10-13, Israel= 1-13
Wireless Guest Network	The Guest SSID (Virtual Access Point) can be enabled by selecting the **Enable Wireless Guest Network** checkbox ☑. Rename the Wireless Guest Network as you wish. **NOTE:** Remote wireless hosts cannot scan Guest SSIDs.

7.2 Security

Security options include authentication and encryption services based on the wired equivalent privacy (WEP) algorithm. WEP is a set of security services used to protect 802.11 networks from unauthorized access, such as eavesdropping; in this case, the capture of wireless network traffic. When data encryption is enabled, secret shared encryption keys are generated and used by the source station and the destination station to alter frame bits, thus avoiding disclosure to eavesdroppers.

802.11 protocols support two types of network authentication services: open system and shared key. Under open system authentication, any wireless station can request authentication. The system that needs to authenticate with another wireless station sends an authentication management frame that contains the identity of the sending station. The receiving station then sends back a frame that indicates whether it recognizes the identity of the sending station. Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

The following screen appears when Security is selected. The options shown here allow you to configure security features of the wireless LAN interface.



Consult the table below for detailed descriptions of the options available.
Click **Save/Apply** to implement new configuration settings.

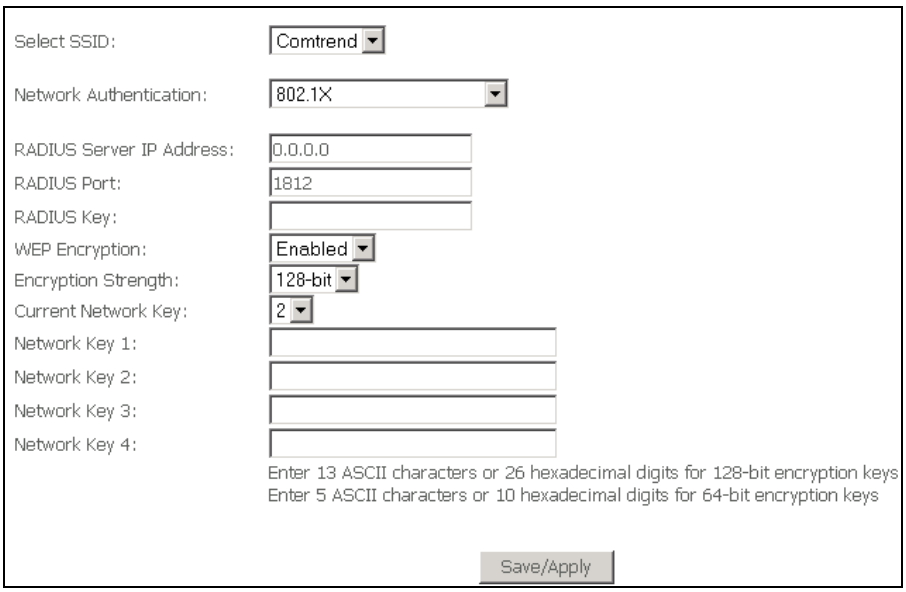
Select SSID

Select the wireless network name from the drop-down box. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.

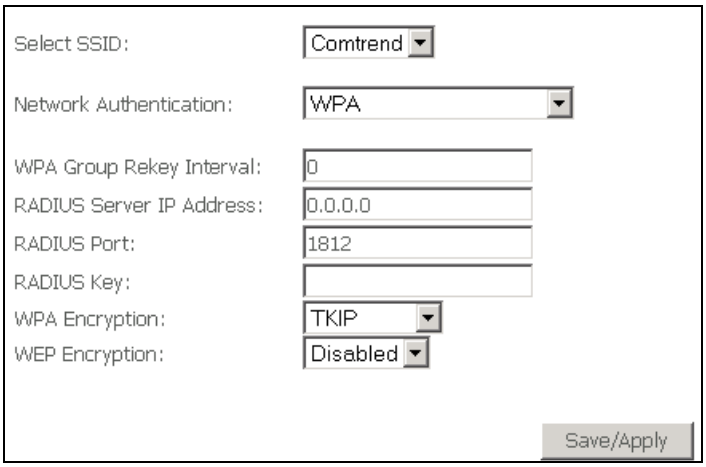
Network Authentication

This option specifies whether a network key is used for authentication to the wireless network. If network authentication is set to Open, then no authentication is provided. Despite this, the identity of the client is still verified.

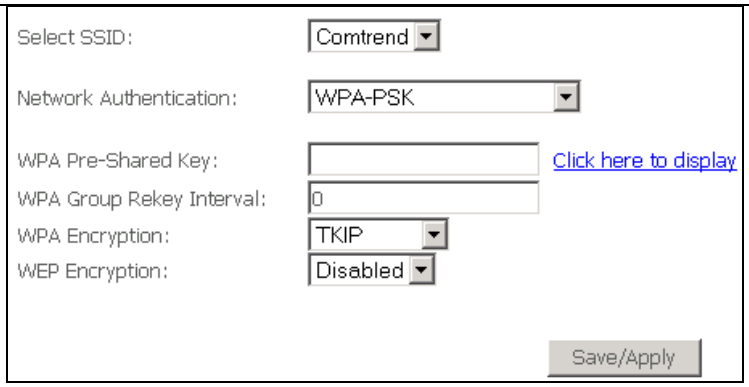
Each authentication type has its own settings. For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and Key fields. WEP Encryption will also be enabled as shown below.



The settings for WPA authentication are shown below.



The settings for WPA-PSK authentication are shown below.



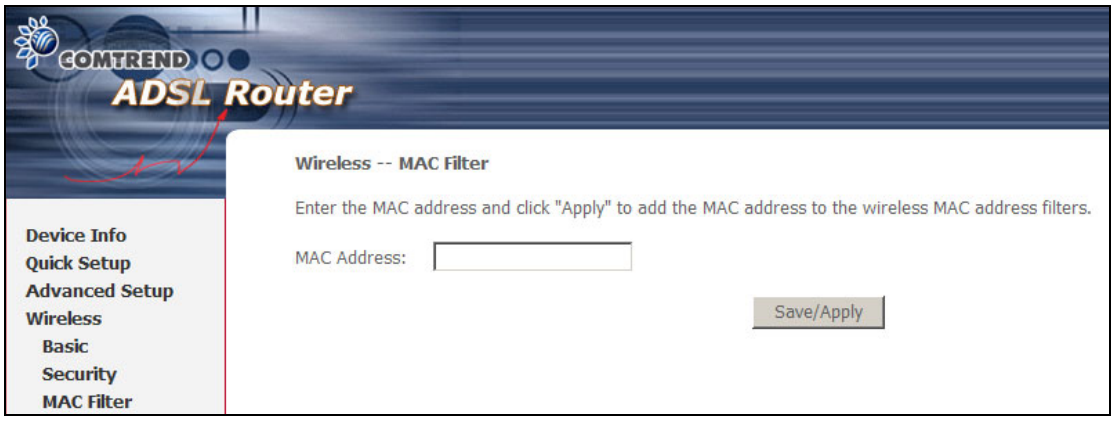
WEP Encryption
This option specifies whether data sent over the network is encrypted. The same network key is used for data encryption and network authentication. Four network keys can be defined although only one can be used at any one time. Use the Current Network Key list box to select the appropriate network key.
Encryption Strength
This drop-down list box will display when WEP Encryption is enabled. The key strength is proportional to the number of binary bits comprising the key. This means that keys with a greater number of bits have a greater degree of security and are considerably more difficult to crack. Encryption strength can be set to either 64-bit or 128-bit. A 64-bit key is equivalent to 5 ASCII characters or 10 hexadecimal numbers. A 128-bit key contains 13 ASCII characters or 26 hexadecimal numbers. Each key contains a 24-bit header (an initiation vector) which enables parallel decoding of multiple streams of encrypted data.

7.3 MAC Filter

This option allows access to the router to be restricted based upon MAC addresses. To add a MAC Address filter, click the **Add** button shown below. To delete a filter, select it from the table below and click the **Remove** button.

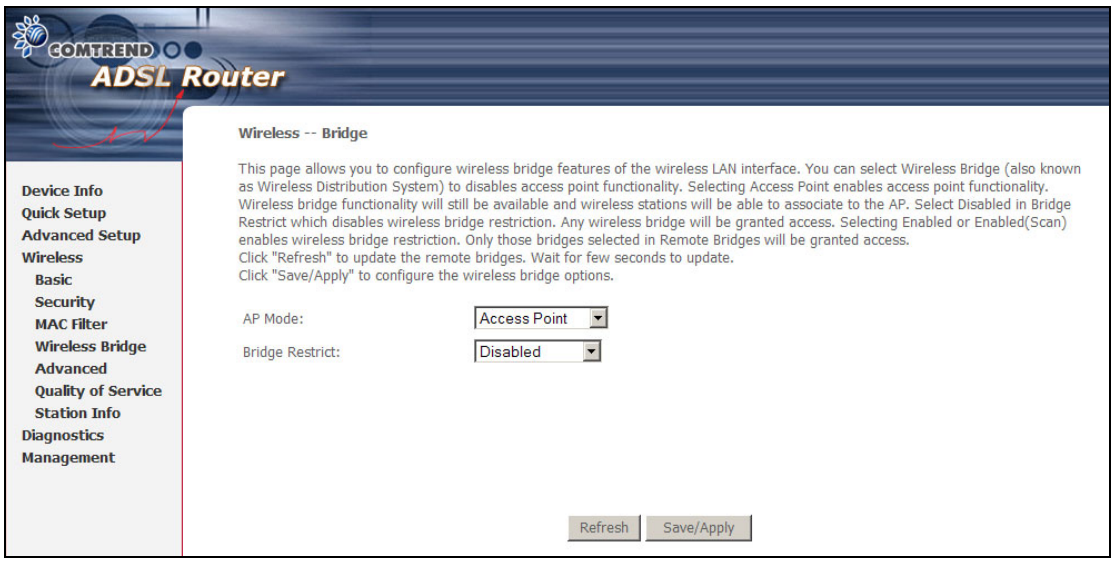
Option	Description
MAC Restrict Mode	Disabled: MAC filtering is disabled. Allow: Permits access for the specified MAC addresses Deny: Rejects access for the specified MAC addresses
MAC Address	Lists the MAC addresses subject to the MAC Restrict Mode. A maximum of 60 MAC addresses can be added. Every network device has a unique 48-bit MAC address. This is usually shown as xx.xx.xx.xx.xx.xx, where xx are hexadecimal numbers.

After clicking the **Add** button, the following screen appears.
Enter the MAC address in the box provided and click **Save/Apply**.



7.4 Wireless Bridge

This screen allows for the configuration of wireless bridge features of the WLAN interface. See the table beneath for detailed explanations of the various options.


COMTREND
ADSL Router
Wireless -- Bridge
This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disables access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.
Click "Refresh" to update the remote bridges. Wait for few seconds to update.
Click "Save/Apply" to configure the wireless bridge options.
AP Mode:
Access Point
Bridge Restrict:
Disabled
Refresh
Save/Apply
Device Info
Quick Setup
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Quality of Service
Station Info
Diagnostics
Management

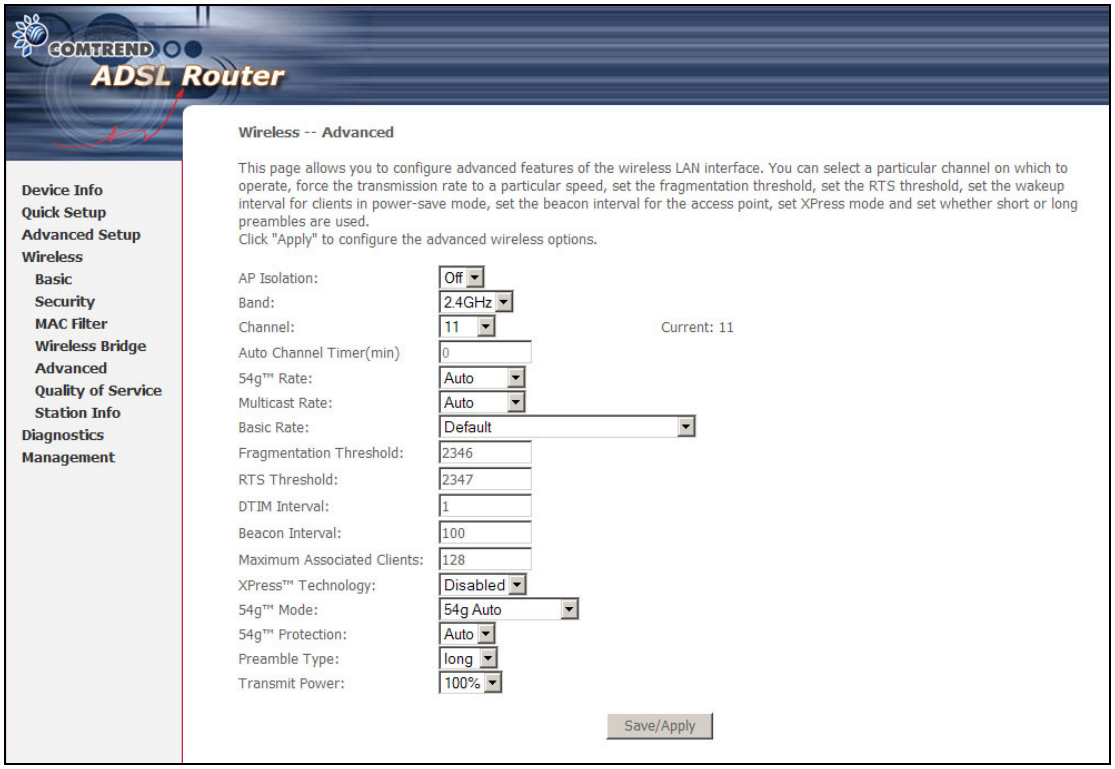
Click **Save/Apply** to implement new configuration settings.

AP Mode	Description
Access Point	Selecting **Wireless Bridge** (aka Wireless Distribution System) disables Access Point (AP) functionality, while selecting **Access Point** enables AP functionality. In **Access Point** mode, wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.
Bridge Restrict	Selecting **Disabled** disables wireless bridge restriction, which means that any wireless bridge will be granted access. Selecting **Enabled** or **Enabled (Scan)** enables wireless bridge restriction. Only those bridges selected in the Remote Bridges list will be granted access. Click **Refresh** to update the station list when Bridge Restrict is enabled.

7.5 Advanced

The Advanced screen allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.

Click **Save/Apply** to set new advanced wireless options.

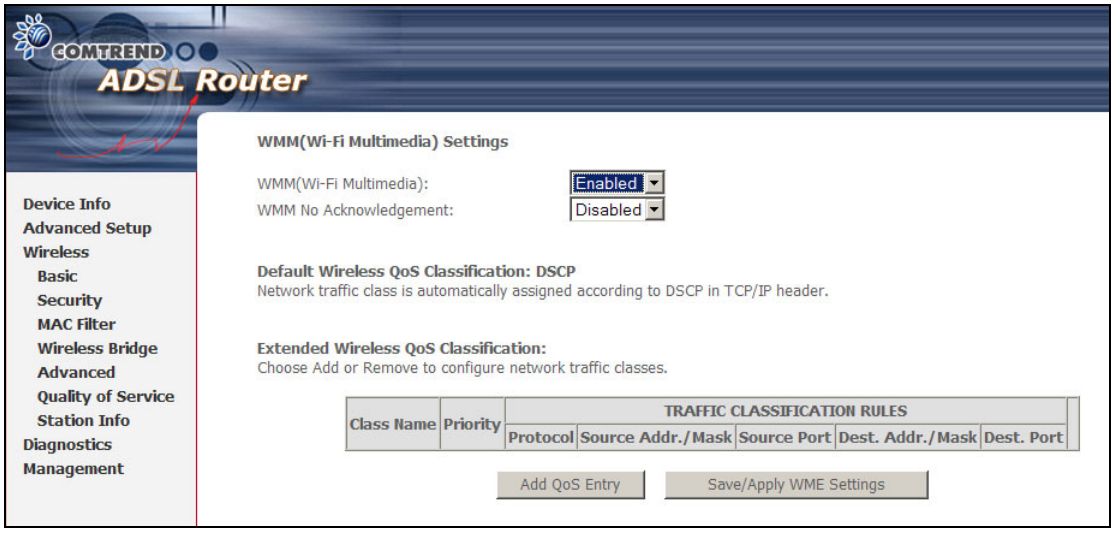

COMTREND
ADSL Router
Device Info
Quick Setup
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Quality of Service
Station Info
Diagnostics
Management
Wireless -- Advanced
This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.
Click "Apply" to configure the advanced wireless options.
AP Isolation: Off
Band: 2.4GHz
Channel: 11 Current: 11
Auto Channel Timer(min) 0
54g™ Rate: Auto
Multicast Rate: Auto
Basic Rate: Default
Fragmentation Threshold: 2346
RTS Threshold: 2347
DTIM Interval: 1
Beacon Interval: 100
Maximum Associated Clients: 128
XPress™ Technology: Disabled
54g™ Mode: 54g Auto
54g™ Protection: Auto
Preamble Type: long
Transmit Power: 100%
Save/Apply

Field	Description
AP Isolation	Select On or Off. By enabling this feature, wireless clients associated with the Access Point can be linked.
Band	The new amendment allows IEEE 802.11g units to fall back to speeds of 11 Mbps, so IEEE 802.11b and IEEE 802.11g devices can coexist in the same network. The two standards apply to the 2.4 GHz frequency band. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a standard, which has a 54 Mbps rate at 5 GHz. (IEEE 802.11a has other differences compared to IEEE 802.11b or g, such as offering more channels.)
Channel	Drop-down menu that allows selection of a specific channel.
Auto Channel Timer (min)	Auto channel scan timer in minutes (0 to disable)
54g Rate	Drop-down menu that specifies the following fixed rates: Auto: Default. Uses the 11 Mbps data rate when possible but drops to lower rates when necessary. 1 Mbps, 2Mbps, 5.5Mbps, or 11Mbps fixed rates. The appropriate setting is dependent on signal strength.
Multicast Rate	Setting for multicast packet transmit rate (1-54 Mbps)
Basic Rate	Setting basic transmission rate.

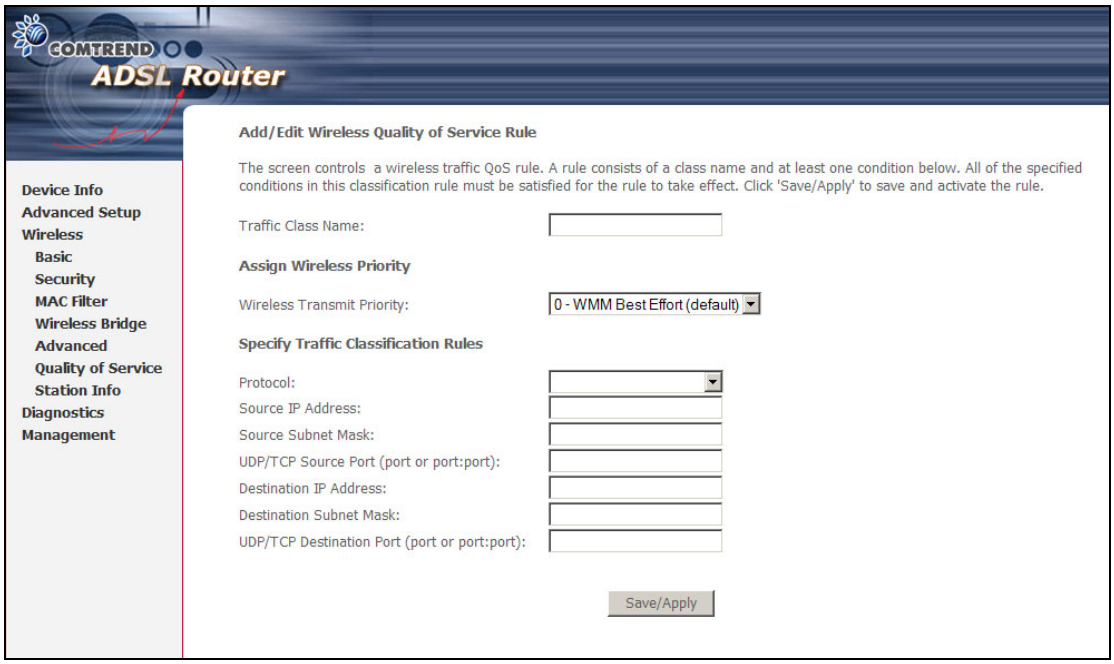
Fragmentation Threshold	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented. Enter a value between 256 and 2346. If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.
RTS Threshold	Request to Send, when set in bytes, specifies the packet size beyond which the WLAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits smaller packet without using RTS/CTS. The default setting of 2347 (maximum length) disables RTS Threshold.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.
Beacon Interval	The amount of time between beacon transmissions in milliseconds. The default is 100 ms and the acceptable range is 1 – 65535. The beacon transmissions identify the presence of an access point. By default, network devices passively scan all RF channels listening for beacons coming from access points. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).
Maximum Associated Clients	The maximum number of clients allowed to connect to the router.
Xpress ™ Technology	Xpress Technology is compliant with draft specifications of two planned wireless industry standards.
54g ™ Mode	Set the mode to 54g Auto for the widest compatibility. Select the mode to 54g Performance for the fastest performance among 54g certified equipment. Set the mode to 54g LRS if you are experiencing difficulty with legacy 802.11b equipment. Select **Auto** mode for greatest compatibility. Select **Performance** mode for the fastest performance among 54g certified equipment. Select **LRS** mode if you are experiencing difficulty with legacy 802.11b equipment. If this does not work, you may also try **802.11b only** mode.
54g Protection	In Auto mode, the router will use RTS/CTS to improve 802.11g performance in mixed 802.11g/802.11b networks. Turning protection **Off** will maximize 802.11g throughput under most conditions.
Preamble Type	Short preamble is intended for applications where maximum throughput is desired but it does not work with legacy equipment. Long preamble works with the current 1 and 2 Mbit/s DSSS specification as described in IEEE Std 802.11-1999
Transmit Power	Set the power output (by percentage) as desired.

7.6 Quality of Service

WMM provides advanced quality of service (QoS) features for Wi-Fi networks to improve the end-user experience by prioritizing audio, video and voice traffic and optimizing the way shared network resources are allocated among competing applications. To enable WMM, select **Enabled** in the WMM (Wi-Fi Multimedia) drop down list box. The screen will display as shown below.



To add an **Extended Wireless QoS Classification**, click **Add QoS Entry**.

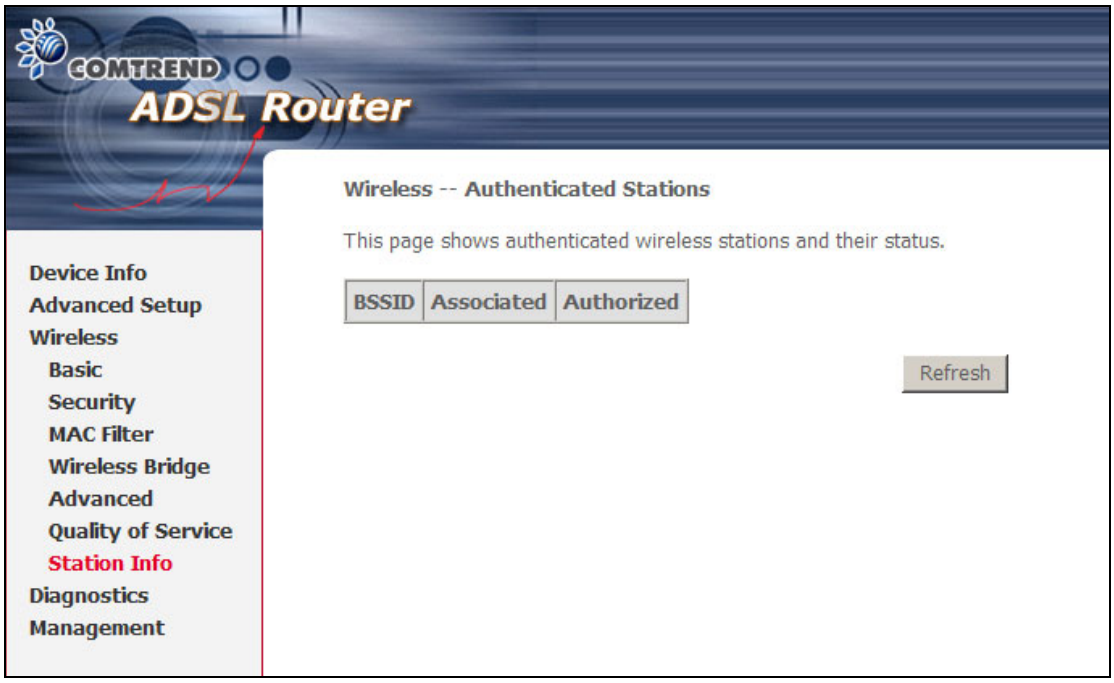

COMTREND
ADSL Router
Device Info
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Quality of Service
Station Info
Diagnostics
Management
Add/Edit Wireless Quality of Service Rule
The screen controls a wireless traffic QoS rule. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.
Traffic Class Name:
Assign Wireless Priority
Wireless Transmit Priority:
0 - WMM Best Effort (default)
Specify Traffic Classification Rules
Protocol:
Source IP Address:
Source Subnet Mask:
UDP/TCP Source Port (port or port:port):
Destination IP Address:
Destination Subnet Mask:
UDP/TCP Destination Port (port or port:port):
Save/Apply

Enter a **Traffic Class Name** and assign the **Wireless Transmit Priority** from the drop-down list box. **Specify Traffic Classification Rules** by choosing the desired parameters under this heading. Click **Save/Apply** to add the Wireless QoS rule.

When finished adding rules, click **Save/Apply WME Settings** on the main screen.

7.7 Station Info

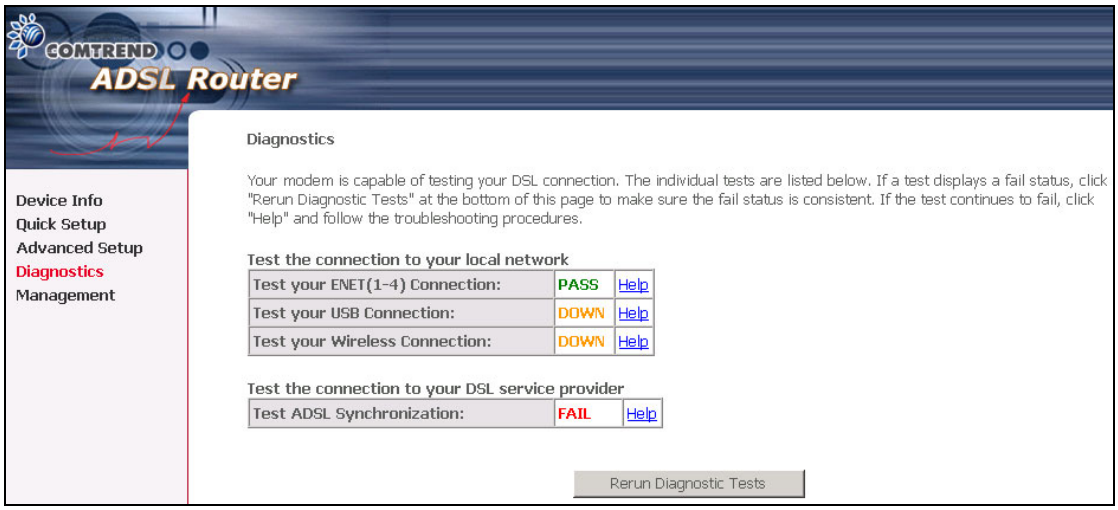
This page shows authenticated wireless stations and their status. Click the **Refresh** button to update the list of stations in the WLAN.



Heading	Description
BSSID	The BSSID is a 48-bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Media Access Control) address of the AP (Access Point); and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Associated	Lists all the stations that are associated with the Access Point, along with the amount of time since packets were transferred to and from each station. If a station is idle for too long, it is removed from this list.
Authorized	Lists those devices with authorized access.

Chapter 8 Diagnostics

The Diagnostics menu provides feedback on the connection status of the device. The individual tests are listed below. If a test displays a fail status, click **Rerun Diagnostic Tests** at the bottom of the screen to retest and confirm the error. If the test continues to fail, click **Help** and follow the troubleshooting procedures.

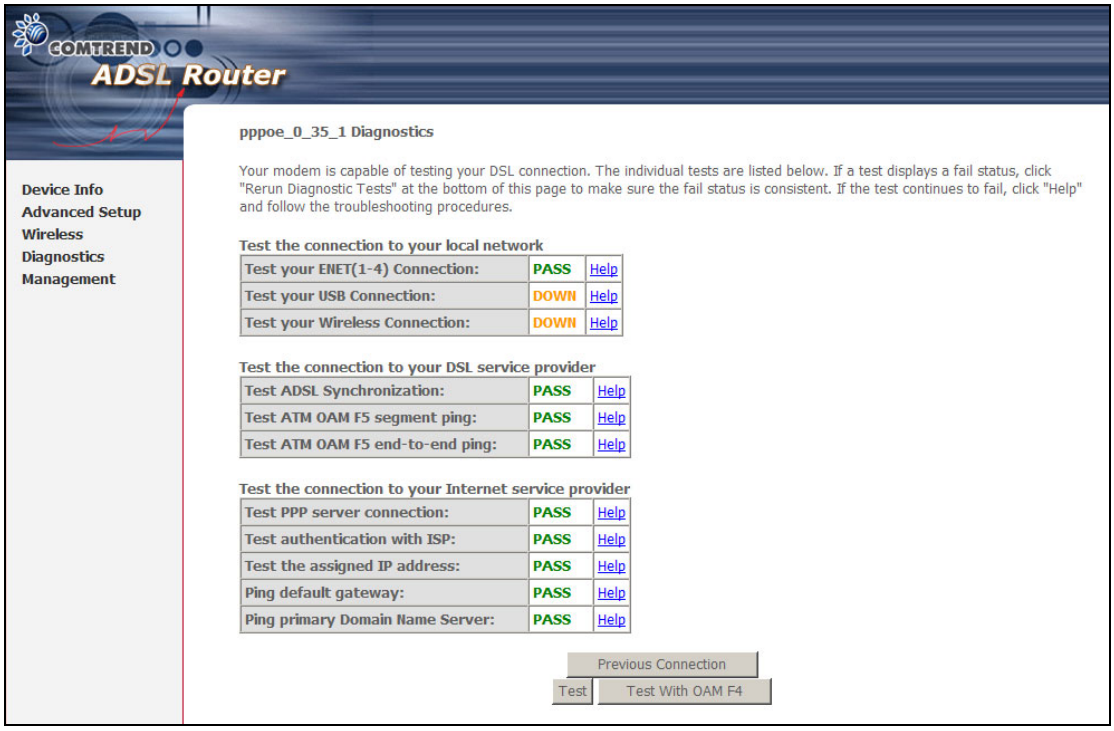

COMTREND
ADSL Router
Device Info
Quick Setup
Advanced Setup
Diagnostics
Management
Diagnostics
Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.
Test the connection to your local network
Test your ENET(1-4) Connection: PASS Help
Test your USB Connection: DOWN Help
Test your Wireless Connection: DOWN Help
Test the connection to your DSL service provider
Test ADSL Synchronization: FAIL Help
Rerun Diagnostic Tests

The basic test set (no PVC configured) is described in the table below. For help with the other tests click on the **Help** link next to the test condition for guidance

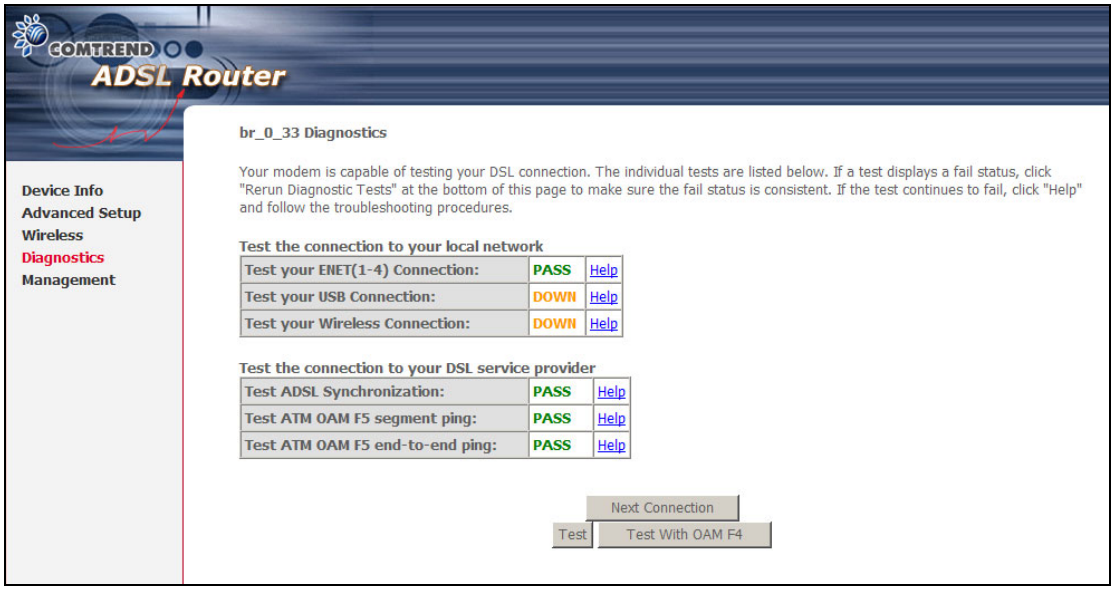
Test	Description
ENET Connection	**Pass:** Indicates that the CT-5361T has detected the Ethernet interface on your computer. **Fail:** Indicates that the CT-5361T does not detect the Ethernet interface on your computer.
USB connection	**Pass:** Indicates that the CT-5361T has detected the USB interface on your computer. **Down:** Indicates that the CT-5361T does not detect the USB interface on your computer.
Wireless connection	**Pass:** Indicates that the CT-5361T has detected the Wireless interface on your computer. **Down:** Indicates that the CT-5361T does not detect the Wireless interface on your computer.
ADSL Synchronization	**Pass:** Indicates that the CT-5361T has detected a DSL signal from the telephone company. **Fail:** Indicates that the CT-5361T does not detect a DSL signal from the telephone company.

Diagnostics screens for various connection types are provided below.

PPPoE Connection


COMTREND
ADSL Router
Device Info
Advanced Setup
Wireless
Diagnostics
Management
pppoe_0_35_1 Diagnostics
Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.
Test the connection to your local network
Test your ENET(1-4) Connection: PASS Help
Test your USB Connection: DOWN Help
Test your Wireless Connection: DOWN Help
Test the connection to your DSL service provider
Test ADSL Synchronization: PASS Help
Test ATM OAM F5 segment ping: PASS Help
Test ATM OAM F5 end-to-end ping: PASS Help
Test the connection to your Internet service provider
Test PPP server connection: PASS Help
Test authentication with ISP: PASS Help
Test the assigned IP address: PASS Help
Ping default gateway: PASS Help
Ping primary Domain Name Server: PASS Help
Previous Connection
Test
Test With OAM F4

Bridge Connection


COMTREND
ADSL Router
Device Info
Advanced Setup
Wireless
Diagnostics
Management
br_0_33 Diagnostics
Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.
Test the connection to your local network
Test your ENET(1-4) Connection: PASS Help
Test your USB Connection: DOWN Help
Test your Wireless Connection: DOWN Help
Test the connection to your DSL service provider
Test ADSL Synchronization: PASS Help
Test ATM OAM F5 segment ping: PASS Help
Test ATM OAM F5 end-to-end ping: PASS Help
Next Connection
Test
Test With OAM F4

Chapter 9 Management

The Management menu has the following maintenance functions and processes:

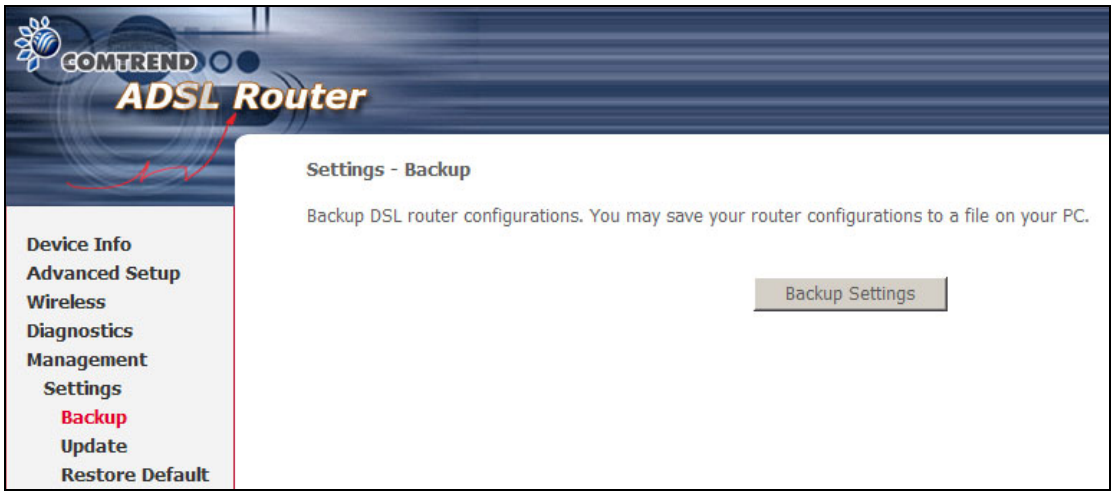
9.1 Settings	9.5 Internet Time
9.2 System Log	9.6 Access Control
9.3 SNMP Agent	9.7 Update Software
9.4 TR-069 Client	9.8 Save and Reboot

9.1 Settings

This includes Backup Settings, Update Settings, and Restore Default screens.

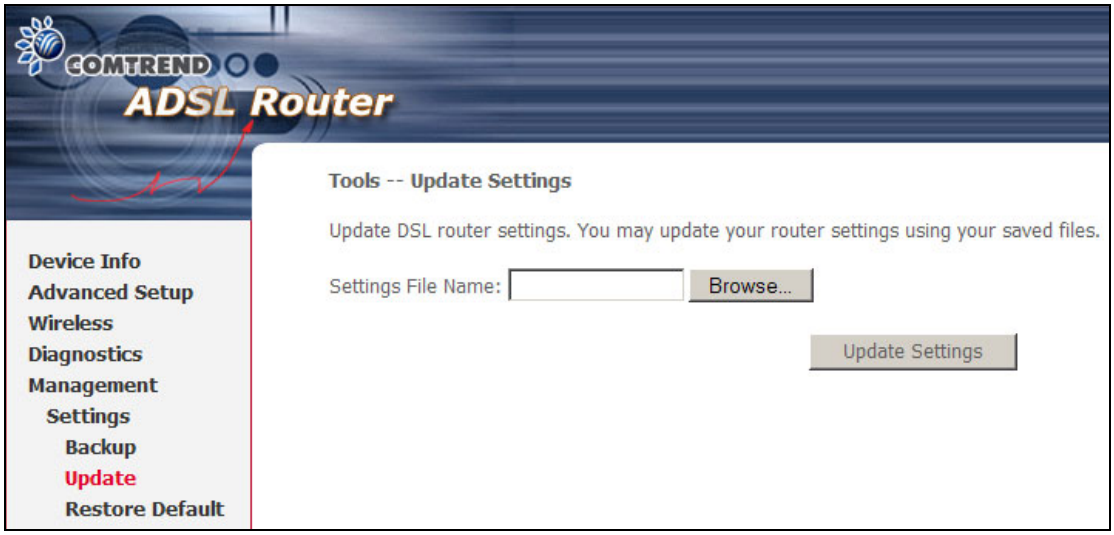
9.1.1 Backup Settings

To save the current configuration to a file on your PC, click **Backup Settings**. You will be prompted for a location of the backup file. This file can later be used to recover settings using the **Update Settings** function described below.



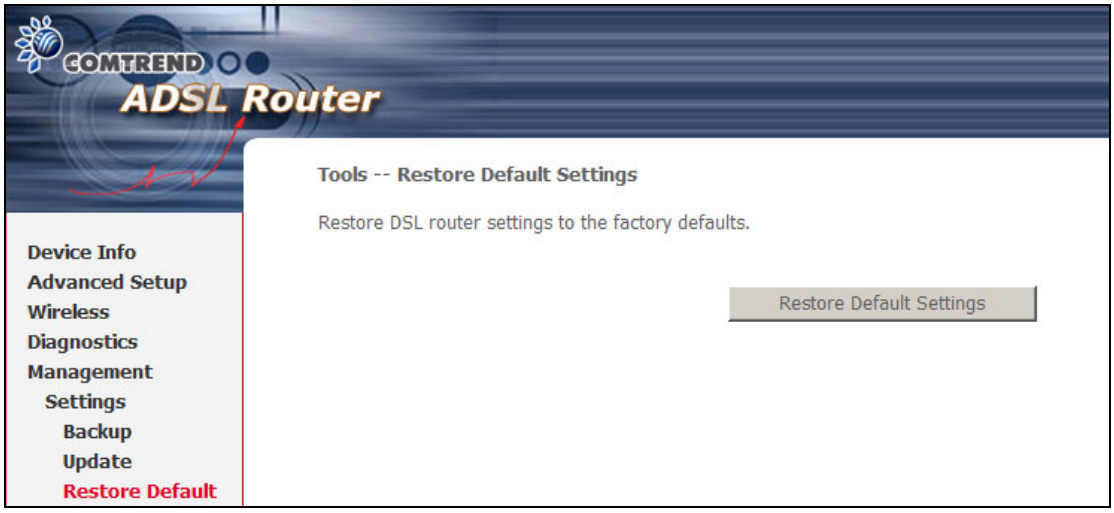
9.1.2 Update Settings

This option recovers configuration files previously saved using **Backup Settings**. Enter the file name (including folder path) in the **Settings File Name** box or press **Browse…** to search for the file. Click **Update Settings** to recover settings.

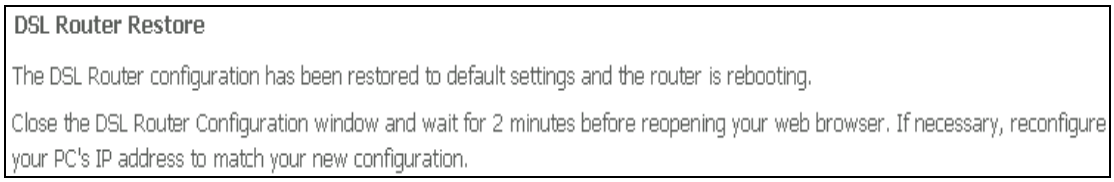


9.1.3 Restore Default

Click **Restore Default Settings** to restore the CT-5361T to factory default settings.



After **Restore Default Settings** is clicked, the following screen appears.


DSL Router Restore
The DSL Router configuration has been restored to default settings and the router is rebooting.
Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

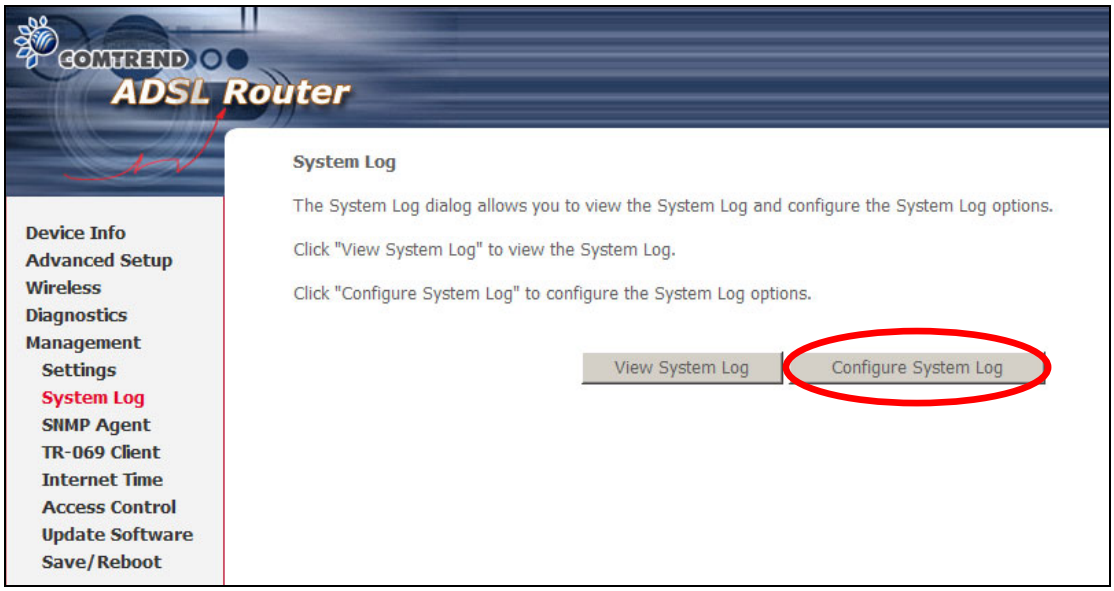
Close the browser and wait for 2 minutes before reopening it. It may also be necessary, to reconfigure your PC IP configuration to match your new settings.

NOTE:	This entry has the same effect as the **Reset** button. The CT-5361T board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for more than 5 seconds, the boot loader will erase the configuration data saved in flash memory.

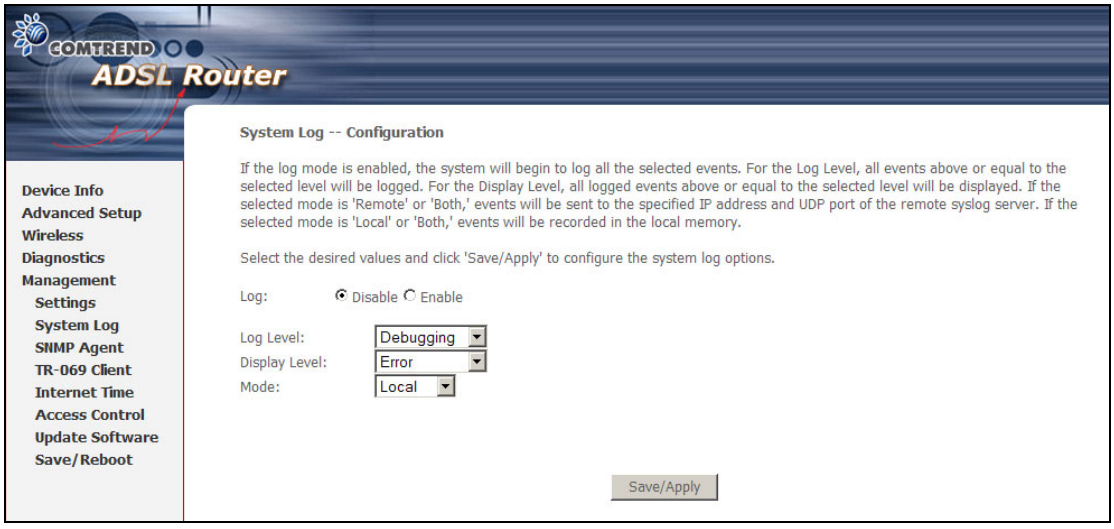
9.2 System Log

This function allows a system log to be kept and viewed upon request.
Follow the steps below to configure, enable, and view the system log.

Step 1: Click **Configure System Log** as shown below.



Step 2: Select desired options and click **Save/Apply**.

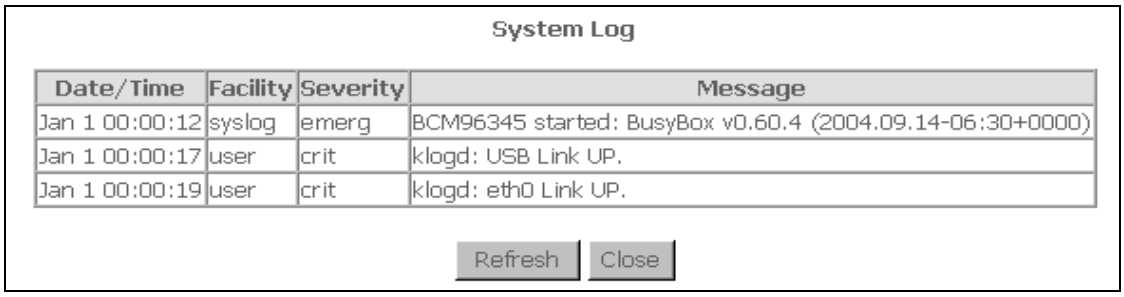

COMTREND
ADSL Router
Device Info
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
SNMP Agent
TR-069 Client
Internet Time
Access Control
Update Software
Save/Reboot
System Log -- Configuration
If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.
Select the desired values and click 'Save/Apply' to configure the system log options.
Log: Disable Enable
Log Level: Debugging
Display Level: Error
Mode: Local
Save/Apply

Consult the table below for detailed descriptions of each system log option.

Option	Description
Log	Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled. To enable it, tick Enable and then Apply button.
Log level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the CT-5361T SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event.

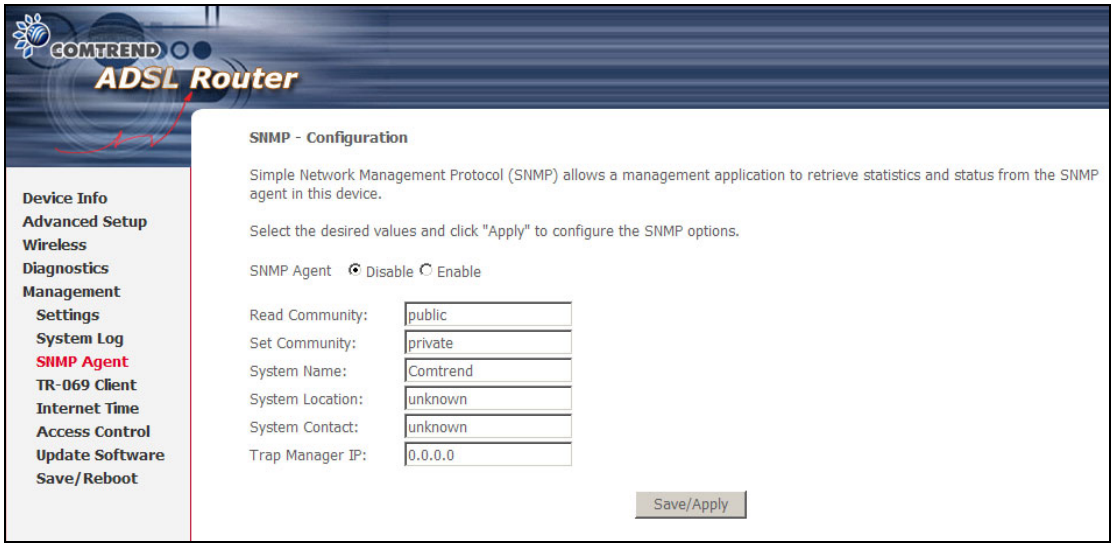
	By default, the log level is "Debugging", which is the lowest critical level. The log levels are defined as follows: • Emergency = system is unusable • Alert = action must be taken immediately • Critical = critical conditions • Error = Error conditions • Warning = normal but significant condition • Notice= normal but insignificant condition • Informational= provides information for reference • Debugging = debug-level messages Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.
Display Level	Allows the user to select the logged events and displays on the **View System Log** window for events of this level and above to the highest Emergency level.
Mode	Allows you to specify whether events should be stored in the local memory, or be sent to a remote system log server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote system log server. When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.

STEP 3: Click **View System Log**. The results are displayed as follows.



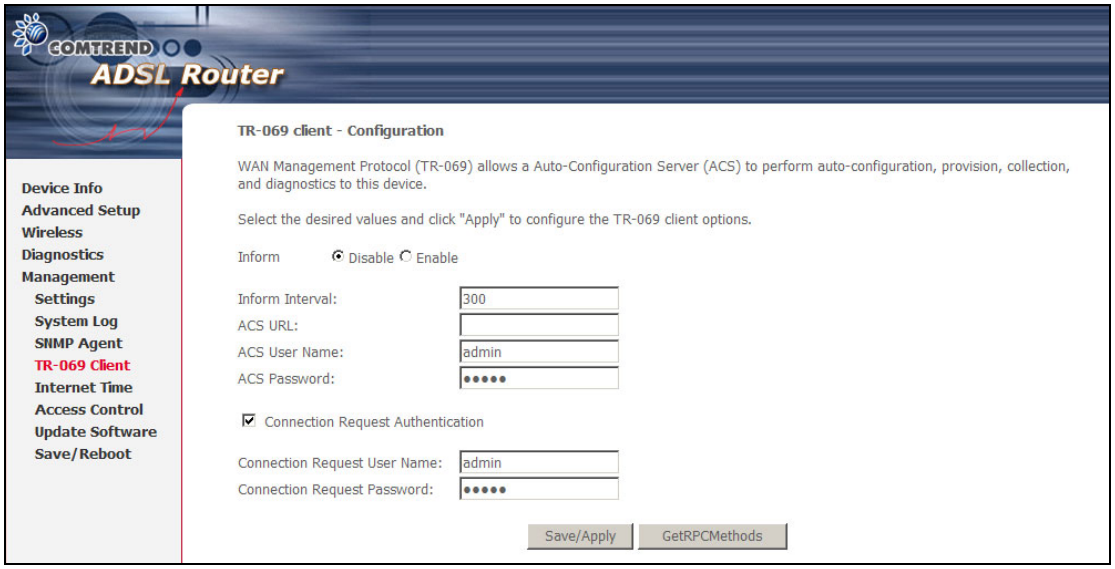
9.3 SNMP Agent

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device. Select the **Enable** radio button, configure options, and click **Save/Apply** to activate SNMP.



9.4 TR-069 Client

WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.



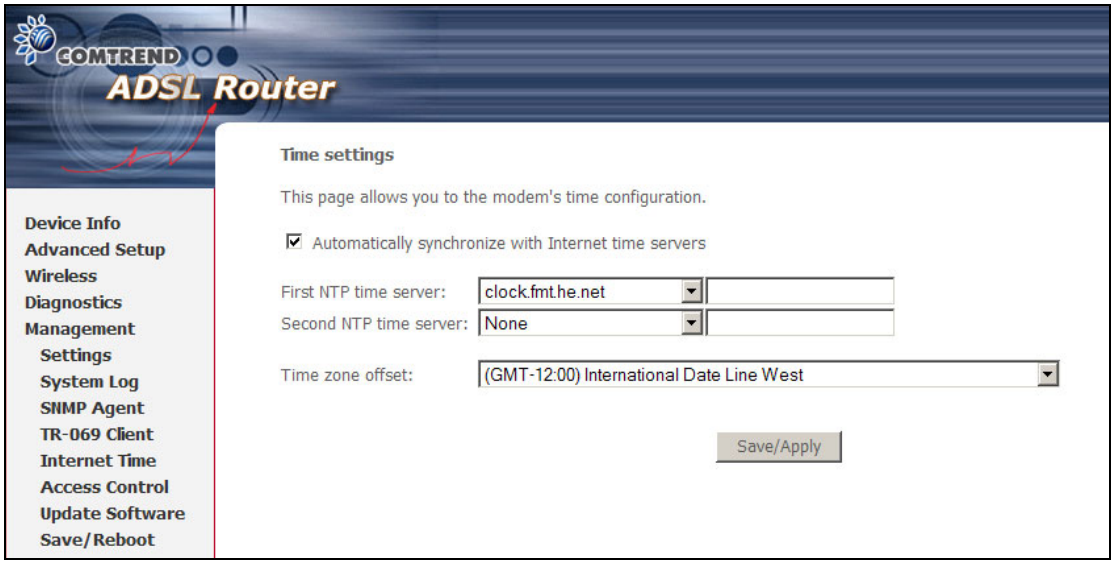
Option	Description
Inform	Disable/Enable TR-069 client on the CPE.
Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method.
ACS URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication.
ACS User Name	Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management

	Protocol. This username is used only for HTTP-based authentication of the CPE.
ACS Password	Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE.
Connection Request	
Authorization	Tick the checkbox ☑ to enable.
User Name	Username used to authenticate an ACS making a Connection Request to the CPE.
Password	Password used to authenticate an ACS making a Connection Request to the CPE.

The **Get RPC Methods** button forces the CPE to establish an immediate connection to the ACS. This may be used to discover the set of methods supported by the ACS or CPE. This list may include both standard TR-069 methods (those defined in this specification or a subsequent version) and vendor-specific methods. The receiver of the response MUST ignore any unrecognized methods.

9.5 Internet Time

This option will automatically synchronize the router time with Internet timeservers. To enable time synchronization, tick the corresponding checkbox ☑, choose your preferred time server(s), select the correct time zone offset, and click **Save/Apply**.

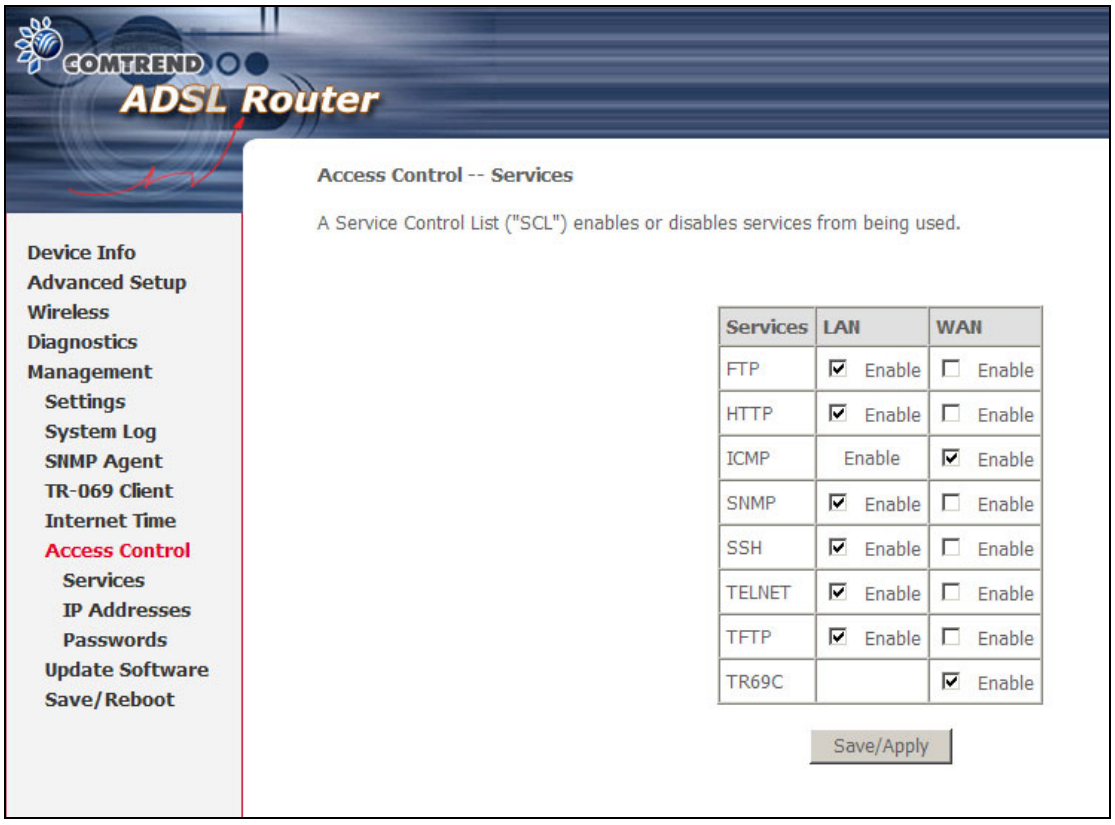


NOTE:	Internet Time must be activated to use Parental Control (page 56). In addition, this menu item is not displayed when in Bridge mode since the router would not be able to connect to the NTP timeserver.

9.6 Access Control

9.6.1 Services

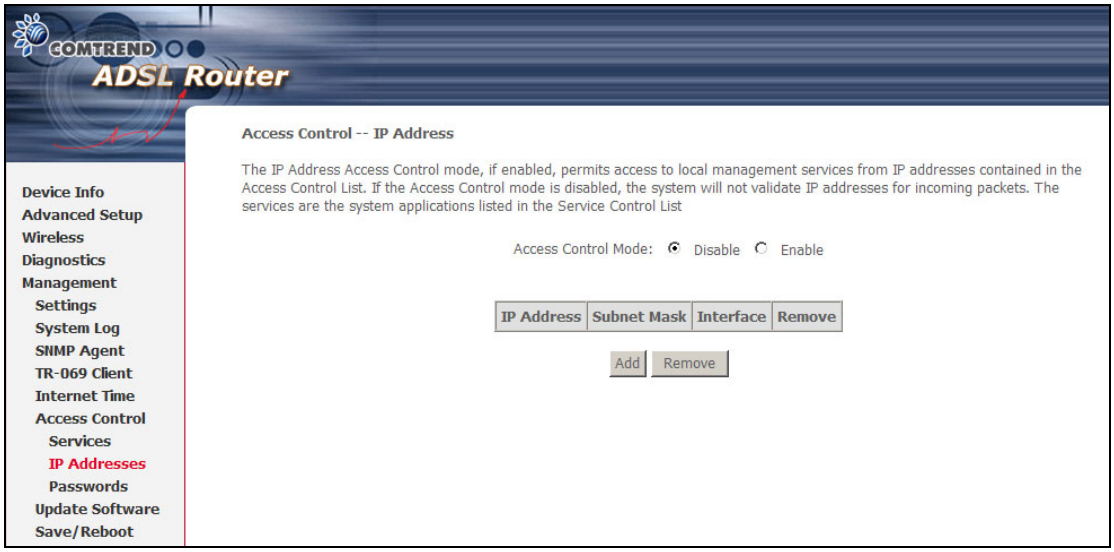
This option controls the access services over the LAN or WAN. These services include FTP, HTTP, ICMP, SNMP, SSH, TELNET, TFTP, and TR69C (TR-069 client). Enable a service by ticking the corresponding checkbox ☑ under LAN or WAN.



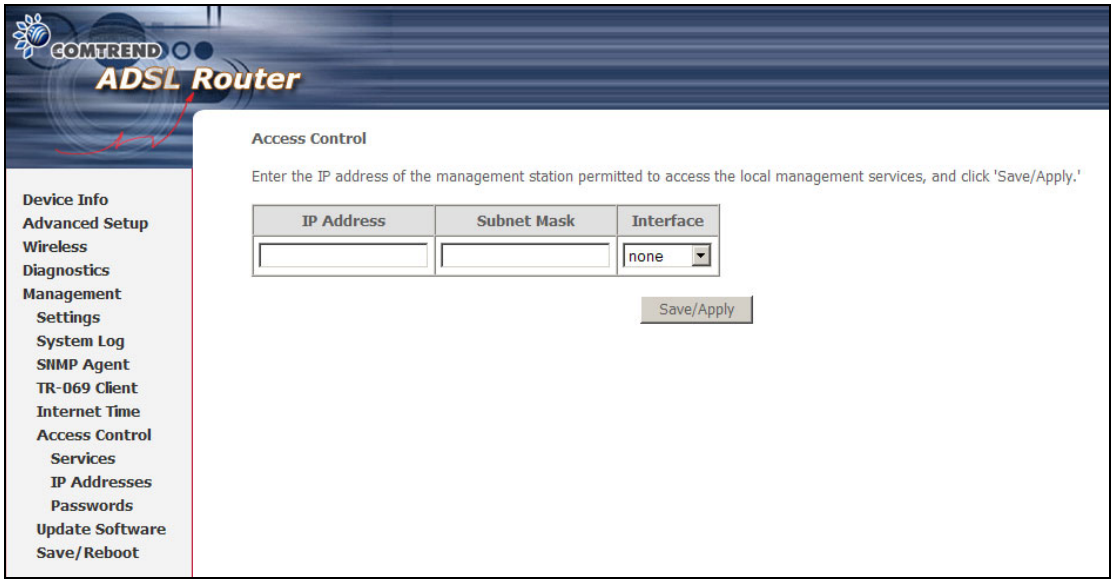
NOTES - 1. The WAN column only appears if a WAN connection is configured.
2. Appendix D: SSH Client contains a quick introduction to SSH clients.

9.6.2 IP Addresses

This option limits access to the router by IP address. When **Access Control Mode** is enabled, only the IP addresses listed here can access the router.



Before enabling **Access Control Mode**, configure the IP addresses by clicking the **Add** button. Enter the IP address and subnet mask, and select an interface. Click **Save/Apply** to add this IP address to the access control list.

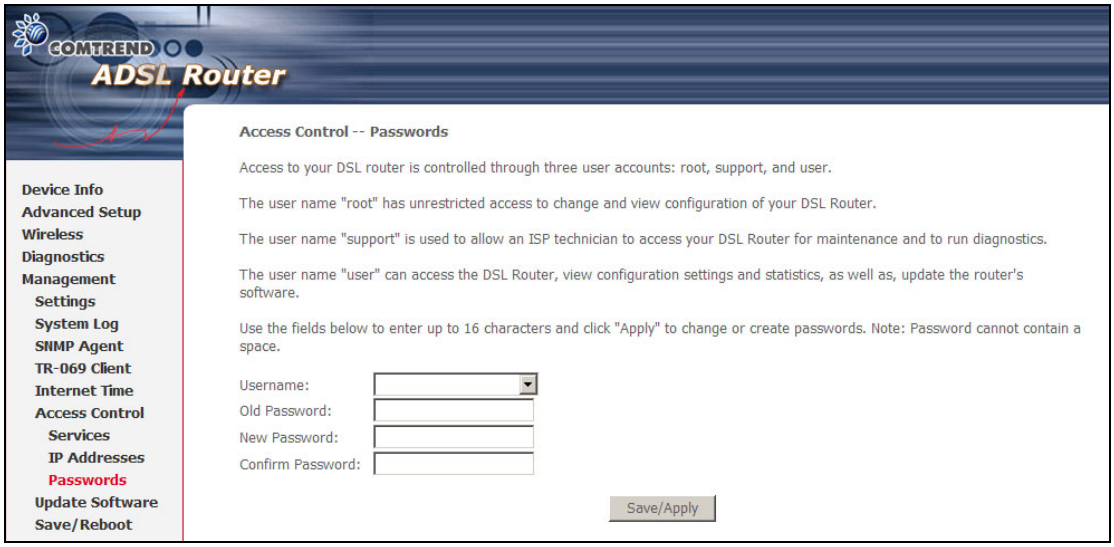


9.6.3 Passwords

This screen is used to configure the user account access passwords for the device. Access to the CT-5361T is controlled through the following three user accounts:

- **root** - this has unrestricted access to change and view the configuration.
- **support** - used for remote maintenance and diagnostics of the router
- **user** - this has limited access. This account can view configuration settings and statistics, as well as, update the router firmware.

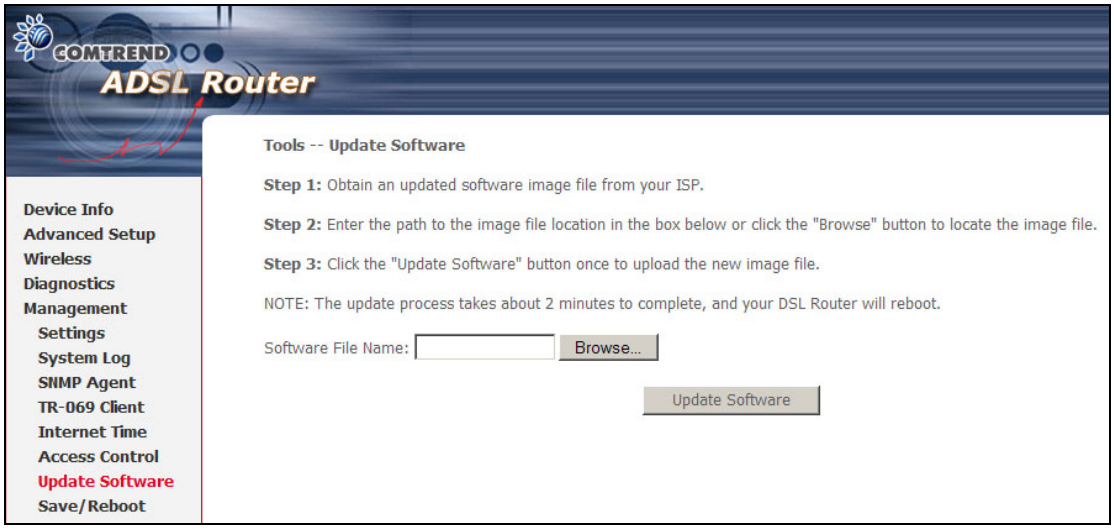
Use the fields below to change password settings. Click **Save/Apply** to continue.


COMTREND
ADSL Router
Device Info
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
SNMP Agent
TR-069 Client
Internet Time
Access Control
Services
IP Addresses
Passwords
Update Software
Save/Reboot
Access Control -- Passwords
Access to your DSL router is controlled through three user accounts: root, support, and user.
The user name "root" has unrestricted access to change and view configuration of your DSL Router.
The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.
The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.
Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.
Username:
Old Password:
New Password:
Confirm Password:
Save/Apply

NOTE: Passwords must be 16 characters or less.

9.7 Update Software

This option allows for firmware upgrades from a locally stored file.


COMTREND
ADSL Router
Device Info
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
SNMP Agent
TR-069 Client
Internet Time
Access Control
Update Software
Save/Reboot
Tools -- Update Software
Step 1: Obtain an updated software image file from your ISP.
Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.
Step 3: Click the "Update Software" button once to upload the new image file.
NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.
Software File Name:
Browse...
Update Software

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path and filename of the firmware image file in the **Software File Name** field or click the **Browse** button to locate the image file.

Step 3: Click the **Update Software** button once to upload and install the file.

NOTE:	The update process will take about 2 minutes to complete. The device will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the **Software Version** at the top of the **Device Info** Summary screen with the firmware version installed, to confirm the installation was successful.

9.8 Save and Reboot

To save the current configuration and reboot the router, click **Save/Reboot**.

NOTE: You may need to close the browser window and wait for 2 minutes before reopening it. It may also be necessary, to reset your PC IP configuration.

Appendix A: Firewall

STATEFUL PACKET INSPECTION
Refers to an architecture, where the firewall keeps track of packets on each connection traversing all its interfaces and makes sure they are valid. This is in contrast to static packet filtering which only examines a packet based on the information in the packet header.

DENIAL OF SERVICE ATTACK
Is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Various DoS attacks the device can withstand are ARP Attack, Ping Attack, Ping of Death, Land, SYN Attack, Smurf Attack, and Tear Drop.

TCP/IP/PORT/INTERFACE FILTER
These rules help in the filtering of traffic at the Network layer (i.e. Layer 3). When a Routing interface is created, **Enable Firewall** must be checked. Navigate to Advanced Setup → Security → IP Filtering.

OUTGOING IP FILTER
Helps in setting rules to DROP packets from the LAN interface. By default, if the Firewall is Enabled, all IP traffic from the LAN is allowed. By setting up one or more filters, specific packet types coming from the LAN can be dropped.

Filter Name: User defined Filter Name.

Protocol: TCP/UDP, TCP, UDP, or ICMP

Source IP Address/Source Subnet Mask:
Packets with the specific "Source IP Address/Source Subnet Mask" combination will be dropped.

Source Port: This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers (portX : portY) will be dropped.

Destination IP Address/Destination Subnet Mask: Packets with the specific "Destination IP Address/Destination Subnet Mask" combination will be dropped.

Destination Port: This can take on either a single port number or a range of port numbers. Packets having a destination port equal to this value or falling within the range of port numbers (portX : portY) will be dropped.

Example 1:

Filter Name	: Out_Filter1
Protocol	: TCP
Source Address	: 192.168.1.45
Source Subnet Mask	: 255.255.255.0
Source Port	: 80
Dest. Address	: NA
Dest. Subnet Mask	: NA
Dest. Port	: NA

This filter will Drop all TCP packets coming from the LAN with IP Address/Subnet Mask of 192.168.1.45/24 having a source port of 80 irrespective of the destination. All other packets will be Accepted.

Example 2:

Filter Name	: Out_Filter2
Protocol	: UDP
Source Address	: 192.168.1.45
Source Subnet Mask	: 255.255.255.0
Source Port	: 5060:6060
Dest. Address	: 172.16.13.4
Dest. Subnet Mask	: 255.255.255.0
Dest. Port	: 6060:7070

This filter will drop all UDP packets coming from the LAN with IP Address / Subnet Mask of 192.168.1.45/24 and a source port range of 5060 to 6060, destined to 172.16.13.4/24 and a destination port range of 6060 to 7070.

INCOMING IP FILTER

Helps in setting rules to ACCEPT packets from the WAN interface. By default, all incoming IP traffic from the WAN is Blocked, if the Firewall is Enabled. By setting up one or more filters, specific packet types coming from the WAN can be Accepted.

Filter Name: User defined Filter Name.

Protocol: TCP/UDP, TCP, UDP, or ICMP

Source IP Address/Source Subnet Mask: Packets with the specific "Source IP Address/Source Subnet Mask" combination will be accepted.

Source Port: This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers(portX : portY) will be accepted.

Destination IP Address/Destination Subnet Mask: Packets with the specific
"Destination IP Address/Destination Subnet Mask" combination will be accepted.

Destination Port: This can take on either a single port number or a range of port numbers. Packets having a destination port equal to this value or falling within the range of port numbers(portX : portY) will be accepted.

The WAN interface on which these rules apply needs to be selected by the user.

Example 1:

Filter Name	: In_Filter1
Protocol	: TCP
Source Address	: 210.168.219.45
Source Subnet Mask	: 255.255.0.0
Source Port	: 80
Dest. Address	: NA
Dest. Sub. Mask	: NA
Dest. Port	: NA
Selected WAN interface	: mer_0_35/nas_0_35

This filter will ACCEPT all TCP packets coming from WAN interface mer_0_35/nas_0_35 with IP Address/Subnet Mask 210.168.219.45/16 having a source port of 80 irrespective of the destination. All other incoming packets on this interface are DROPPED.

Example 2:

Filter Name	: In_Filter2
Protocol	: UDP
Source Address	: 210.168.219.45
Source Subnet Mask	: 255.255.0.0
Source Port	: 5060:6060
Dest. Address	: 192.168.1.45
Dest. Sub. Mask	: 255.255.255.0
Dest. Port	: 6060:7070

This rule will ACCEPT all UDP packets coming from WAN interface mer_0_35/nas_0_35 with IP Address/Subnet Mask 210.168.219.45/16 and a source port in the range of 5060 to 6060, destined to 192.168.1.45/24 and a destination port in the range of 6060 to 7070. All other incoming packets on this interface are DROPPED.

MAC LAYER FILTER

These rules help in the filtering of Layer 2 traffic. MAC Filtering is only effective on ATM PVCs configured in Bridge mode. After a Bridge mode PVC is created, navigate to Advanced Setup → Security → MAC Filtering in the WUI.

Global Policy: When set to Forwarded the default filter behavior is to Forward all MAC layer frames except those explicitly stated in the rules. Setting it to Blocked changes the default filter behavior to Drop all MAC layer frames except those explicitly stated in the rules.

Protocol Type: PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, or IGMP.

Destination MAC Address: Of the form, XX:XX:XX:XX:XX:XX. Frames with this particular destination address will be Forwarded/Dropped depending on whether the Global Policy is Blocked/Forwarded.

Source MAC Address: Of the form, XX:XX:XX:XX:XX:XX. Frames with this particular source address will be Forwarded/Dropped depending on whether the Global Policy is Blocked/Forwarded.

Frame Direction: (Select an interface on which this rule is applied)

LAN <=> WAN	= All Frames coming/going to/from LAN or to/from WAN.
WAN => LAN	= All Frames coming from WAN destined to LAN.
LAN => WAN	= All Frames coming from LAN destined to WAN

Example 1:

Global Policy	: Forwarded
Protocol Type	: PPPoE
Dest. MAC Address	: 00:12:34:56:78:90
Source MAC Address	: NA
Frame Direction	: LAN => WAN
WAN Interface Selected	: br_0_34/nas_0_34

Addition of this rule drops all PPPoE frames going from LAN to WAN with a Destination MAC Address of 00:12:34:56:78:90 irrespective of its Source MAC Address on the br_0_34 WAN interface. All other frames on this interface are forwarded.

Example 2:

Global Policy	: Blocked
Protocol Type	: PPPoE
Dest. MAC Address	: 00:12:34:56:78:90
Source MAC Address	: 00:34:12:78:90:56
Frame Direction	: WAN => LAN
WAN Interface Selected	: br_0_34/nas_0_34

Addition of this rule forwards all PPPoE frames going from WAN to LAN with a Destination MAC Address of 00:12:34:56:78 and Source MAC Address of 00:34:12:78:90:56 on the br_0_34 WAN interface. All other frames on this interface are dropped.

DAYTIME PARENTAL CONTROL

This feature restricts access of a selected LAN device to an outside Network through the CT-5361T, as per chosen days of the week and the chosen times.

User Name: Name of the Filter.

Browser's MAC Address: Displays MAC address of the LAN device on which the browser is running.

Other MAC Address: If restrictions are to be applied to a device, other than the one on which the browser is running, the MAC address of that LAN device is entered.

Days of the Week: Days when the restrictions are applied.

Start Blocking Time: The time when restrictions on the LAN device begin.

End Blocking Time: The time when restrictions on the LAN device end.

Example:

User Name	: FilterJohn
Browser's MAC Address	: 00:25:46:78:63:21
Days of the Week	: Mon, Wed, Fri
Start Blocking Time	: 14:00
End Blocking Time	: 18:00

With this rule, a LAN device with MAC Address of 00:25:46:78:63:21 will have no access to the WAN on Mondays, Wednesdays, and Fridays, from 2pm to 6pm. On all other days and times, this device will have access to the outside Network.

Appendix B: Pin Assignments

LINE PORT (RJ11)

Pin	Definition	Pin	Definition
1	-	4	ADSL_TIP
2	-	5	-
3	ADSL_RING	6	-

LAN Port (RJ45)

Pin	Definition	Pin	Definition
1	Transmit data+	5	NC
2	Transmit data-	6	Receive data-
3	Receive data+	7	NC
4	NC	8	NC

Appendix C: Specifications

Hardware Interface

RJ-11 X1 for ADSL2+, RJ-45 X 4 for LAN, USB X 1 for LAN, Reset Button X 1, Power Button X 1, Power Jack X 1, WiFi Antenna X 1

WAN Interface

ITU-T G.994.1/G.992.5/G.992.3/G.992.2/G.992.1, ANSI T1.413 Issue 2

G.992.5 (ADSL2+) .....Downstream : 24 Mbps Upstream : 1.3 Mbps
G.992.3 (ADSL2).....Downstream : 12 Mbps Upstream : 1.3 Mbps
Auto-negotiation rate adaptation
G.DMT / G.lite
Annex M

LAN Interface

Standard.....IEEE 802.3, IEEE 802.3u
10/100 BaseT .....Auto-sense
MDI/MDX support.....Yes

WLAN Interface

Standard IEEE802.11b/g
Encryption.....64/128-bit Wired Equivalent Privacy (WEP)
Channels.....11 (US, Canada)/ 13 (Europe)/ 14 (Japan)
Data Rate.....Up to 54Mbps
WPA/WPA2 .....Yes
IEEE 802.1x .....Yes
WMM .....Yes
Optional.....Afterburner mode (Turbo mode)

ATM Attributes

RFC 2684 (RFC 1483) Bridge/Route; RFC 2516 (PPPoE);
RFC 2364 (PPPoA); RFC 1577 (IPoA)

PVCs 16
AAL type AAL5
ATM service class .....UBR/CBR/VBR
ATM UNI support.....UNI3.1/4.0
OAM F4/F5 .....Yes

Management

Compliant with TR-069/TR-098/TR-111 remote management protocols, SNMP, Telnet, Web-based management, Configuration backup and restoration, Software upgrade via HTTP / TFTP / FTP server

Bridge Functions

Transparent bridging and learning .....IEEE 802.1d
VLAN support .....Yes
Spanning Tree Algorithm .....Yes
IGMP Proxy/Snooping .....Yes

Routing Functions

Static route, RIP v1/v2, NAT/PAT, DMZ, DHCP Server/Relay/Client, DNS Proxy, ARP, IGMP Proxy/Snooping

Security Functions

Authentication protocol : PAP, CHAP
VPN : PPTP/L2TP/IpSec pass-through

TCP/IP/Port filtering rules, SSH, Port Triggering/Forwarding, Packet and MAC address filtering, Access Control

Application Passthrough

PPTP, L2TP, IPSec, VoIP, Yahoo messenger, ICQ, RealPlayer, NetMeeting, MSN, X-box

QoS .....L3 policy-based QoS, IP QoS, ToS

USB driver OS Support .....Windows Vista/2000/XP/ME/98SE

Power Supply .....Input: 100 - 240 Vac
Output: 16.5 Vac / 850 mA

Environment Condition

Operating temperature .....0 ~ 50 degrees Celsius
Relative humidity .....5 ~ 95% (non-condensing)

Dimensions .....205 mm (W) x 48 mm (H) x 145 mm (D)

Kit Weight

(1*CT-5361T, 1*RJ11 cable, 1*RJ45 cable, 1*USB cable, 1*Power Adapter, 1*CD-ROM) = 1.3 kg

Certifications..... FCC Part 15 class B, FCC Part 68

NOTE: Specifications are subject to change without notice

Appendix D: SSH Client

Unlike Microsoft Windows, Linux OS has a ssh client included. For Windows users, there is a public domain one called "putty" that can be downloaded from here:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

To access the ssh client you must first enable SSH access for the LAN or WAN from the Management → Access Control → Services menu in the web user interface.

To access the router using the Linux ssh client

For LAN access, type: ssh -l root 192.168.1.1

For WAN access, type: ssh -l support *WAN IP address*

To access the router using the Windows "putty" ssh client

For LAN access, type: putty -ssh -l root 192.168.1.1

For WAN access, type: putty -ssh -l support *WAN IP address*

NOTE: The *WAN IP address* can be found on the Device Info → WAN screen